

تطورات الذكاء الاصطناعي ومقتضيات حماية الحقوق والحريات الأساسية



منظمة العالم الإسلامي للتربية والعلوم والثقافة
ISLAMIC WORLD EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
ORGANISATION DU MONDE ISLAMIQUE POUR L'EDUCATION, LES SCIENCES ET LA CULTURE

تطورات الذكاء الاصطناعي ومقتضيات حماية الحقوق والحريات الأساسية

إدارة الشؤون القانونية بمنظمة الإيسيسكو
تحت إشراف : الأستاذ محمد الهادي السهيلي

الفهرس

المقدمة.. 7

المحور الأول :
استخدام الذكاء الاصطناعي لمواجهة فيروس كورونا 9

المحور الثاني :
الأطر القانونية الدولية لحماية الخصوصية.................................. 21

المحور الثالث :
تحديات التأطير القانوني لحماية البيانات الشخصية
في استخدامات الذكاء الاصطناعي ـ التجارب والاجتهادات ـ 49

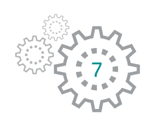
الخاتمة : هل حان موعد وداع الخصوصية ؟.............................. 59



المقدمة

تعرف استعمالات الذكاء الاصطناعي نمواً هائلا نظراً لما توفره من فرص كبيرة وواعدة، خصوصا في قدرتها على التعلم الآلي Machine Learning وكفاءتها التنبؤيّة العالية، استعمالات تنبهت لها العديد من المؤسسات والحكومات ما دفعها للعمل من أجل الانتفاع من مزاياها قدر المستطاع، مثال ذلك عمليات الأداء والدفع، وتنظيم السير والطائرات ذات التحكم عن بُعد، والأَسْوِرة المشفرة سريعة الاستجابة، وتقنيات تمييز الوجوه والتطبيقات الذكية على الهواتف وغيرها.

يوازي هذا الاستعمال المتعاظم للذكاء الاصطناعي تزايد الشكوك حول قدرة هذه التقنية على حماية البيانات الشخصية، نظرا للحاجة الدائمة لخوارزميات الذكاء الاصطناعي إلى مدخلات مستمرة من البيانات وإلى تغذية وتحديث وتدريب دائم، وتتغذى هذه الخوارزميات على كم هائل من المعلومات والبيانات التجريبية المبنية على الحياة الواقعية المستقاة من خبرات البشر ووعيهم وتفاعلهم مع هذه التقنية الحديثة، ما يعني اطلاعها على البيانات الشخصية للأشخاص وبياناتهم الخاصة بُغية معالجتها وتحليلها، فإلى أي حد ساهم الذكاء الاصطناعي في مواجهة جائحة كوفيد 19 ؟ وما هي الآثار التي خلفها فيما يتعلق بالحقوق والحريات الأساسية ؟ وما هي محددات التنظيم القانوني الجيد الكفيل بالحد من آثار الذكاء الاصطناعي على الحقوق والحريات ؟.



المحور الأول: استخدامات الذكاء الاصطناعي لمواجهة فيروس كورونا

أصاب انتشار فيروس كورونا (كوفيد 19) العالم أجمع بصدمة كبرى، فما إن أعلنت الحكومة الصينية عن أول حالة إصابة حتى اجتاح الوباء العالم في فترة وجيزة، وتسبب هذا في شبه شلل تام لكل المجالات (التعليم، المواصلات الدولية، التجارة والاقتصاد...)، بالإضافة إلى حصده مئات الآلاف من الضحايا حول العالم، ووجد الإنسان نفسه عاجزا أمام هذا الوباء الذي عم البشرية، وها نحن الآن أمام أكبر تحدّ يواجهه البشر خلال القرن 21 من حيث انتشاره الجغرافي وإضراره بكل القطاعات البشرية وعلى رأسها القطاعات الاقتصادية والاجتماعية، مما دفع بحكومات الدول والمنظمات الدولية المعنية أن تسابق الزمن من أجل السيطرة على هذه الجائحة من أجل إيجاد حلول للآثار المترتبة عن الأزمة عبر توظيف مختلف الإمكانات البشرية والمادية المتاحة، وتعمل البشرية اليوم جاهدة عبر حكوماتها وصناع قرارها، بالتعاون مع القطاع الخاص، من أجل الاستعانة بتقنيات الذكاء الاصطناعي لمواجهة انتشار وباء كوفيد 19، بغرض تسريع تطوير أدوات الاختبار والمراقبة والتتبع والعلاج، قصد توفير معلومات لحظية ومحيّنة للمواطنين حول تطورات الوباء وسبل الوقاية منه.

I. تنوع استخدامات الذكاء الاصطناعي للحد من انتشار مرض COVID-19

تتم الاستعانة اليوم بتقنيات الذكاء الاصطناعي كأداة فعالة لمكافحة هذه الجائحة، وذلك من خلال استعمال تطبيقات تعتمد على التعلم الآلي (Machine Learning)، ومعالجة اللغات الطبيعية (Natural Languages Processing) والبيانات الضخمة (Big DATA) وذلك من أجل تتبع انتشار الوباء والتشخيص المبكر للمصابين وتسريع عملية



اكتشاف العلاج[1]، وتتجلّى أهمّ استخدامات الذكاء الاصطناعي في أربعة وظائف أساسية :

• التنبؤ

من أهم الأمور التي تم تطويرها عبر الذكاء الاصطناعي هي القدرة على التنبؤ بالأمراض، وذلك من خلال استخدام الخوارزميات والتعلم الآلي (ML)، الذي يتيح التنبؤ بالحالات المستقبلية ورصدها وتصنيفها، وتصبح هذه الإمكانية فعالة إلى حد كبير عندما تتوفر بيانات مكثفة وسليمة وذات جودة، ويعتبر الإعلان الذي قامت به شركة «BlueDot» الكندية، التي رصدت تفشي فيروس كورونا في ووهان عاصمة مقاطعة «خوبي» في الصين في 31 من ديسمبر 2019، حين حذرت من إمكانية الانتشار السريع لهذا المرض دوليا عبر السفر الجوي التجاري، كما قامت بنشر لائحة بالمدن التي من الممكن أن تكون في طليعة المتضررين من الانتشار العالمي للمرض[2]، هذه المنصات المتطورة التي تعمل على توقع حدوث خطر انتشار الأمراض المعدية ونشر إنذارات مبكرة سيكون لها دور كبير مستقبلا في الاستعداد المبكر لمحاصرة مثل هذه الأمراض قبل انتشارها.

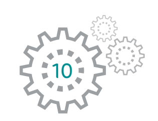
• التشخيص والعلاج

بالإضافة إلى التنبؤ بمسار الوباء، يأمل الكثيرون في أن يساعد الذكاء الاصطناعي في رصد الأشخاص المصابين بما له من إمكانات هامّة في هذا المجال نظرا لقدرة نماذج التعلم الآلي على فحص الصور الطبية والتقاط العلامات المبكرة للمرض، وهي استعمالات يتم توظيفها اليوم في أمراض العيون وأمراض القلب والسرطان، رغم أن هذه النماذج تتطلب عادة الكثير من البيانات[3].

1. Artificial Intelligence against COVID-19: An Early Review. Medium. (2020). Retrieved 24 April 2020, from https://towardsdatascience.com/artificial-intelligence-against-covid-19-an-early-review-92a8360edaba.

2. Pneumonia of unknown aetiology in Wuhan, China: potential for international spread via commercial air travel,Journal of Travel Medicine, Volume 27, Issue 2, March 2020, https://academic.oup.com/jtm/article/27/2/taaa008/5704418.

3. https://ai-forum.com/opinion/ai-could-help-with-the-next-pandemic-but-not-with-this-one/.



أما فيما يتعلق بتشخيص وباء COVID-19، فهو يعتمد على المعايير التالية : الأعراض السريرية التي تشمل أعراض الجهاز التنفسي والحمى والسعال الجاف والالتهاب الرئوي، كما يعتمد على صور الأشعة المقطعية الإيجابية، وكذلك اختبارات الحمض النووي للحالات المصابة بالفيروس، وهي اختبارات تستغرق الكثير من الوقت مع نتائج سلبية كثيرة[4].

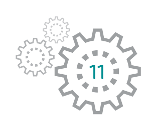
وتتطلب محاصرة فيروس كورونا إجراء العديد من الاختبارات لأجل رصد المصابين، وهو الأمر الذي لا توفره الإمكانات المخبرية المعتمدة في العديد من المؤسسات الصحية، وظهرت عديد من التجارب لهذا الغرض من أجل تطوير تقنيات تمكّن من التشخيص السريع والدقيق للمرض، منها تقنيات الذكاء الاصطناعي لأجل تطوير ما يسمى بـ COVID-Net لتشخيص مرض COVID-19، أنشأها عالمان من جامعة «Waterloo» بالتعاون مع شركة «Darwin AI» في كندا، وتَستخدم هذه الأداة تقنية الشبكات العصبية (Neural Networks)، ويسعى مطوروها لحثّ العلماء على التعاون في تطوير نظام ذكاء اصطناعي يمكن من خلاله تحديد أعراض فيروس كورونا بدقةٍ في صور أشعة الصدر[5].

كما يتم توظيف تقنية الذكاء الاصطناعي في إنشاء تطبيقات ومواقع بقياس احتمال الإصابة بالفيروس من خلال الإجابة على عدد من الأسئلة، لتقوم خوارزميات الحاسوب بتقييم وضع الشخص المعني وتقدم له التشخيص المناسب بناء على أجوبته.

ولابد من أجل محاصرة الوباء من التواصل مع الحالات المشتبه في إصابتها، كما يمكن إنقاذ العديد من الضحايا عبر اتخاذ إجراءات مستعجلة وضمان التدخل الطبي السريع قبل ظهور الأعراض الحادة ومحاولة الحد منها، كما أن المراقبة المستمرة لتطور المرض تُسهم في تعزيز البيانات والمعلومات المتوفرة حوله.

4. Shuai Wangand athers," A deep learning algorithm using CT images to screen for Corona Virus Disease (COVID-19)", https://www.medrxiv.org/content/10.1101/2020.02.14.20023028v5.full.pdf+html.

5. Artificial Intelligence against COVID-19: An Early Review. Medium. (2020). Retrieved 24 April 2020, from https://towardsdatascience.com/artificial-intelligence-against-covid-19-an-early-review-92a8360edaba.



كما تمت الاستعانة ببرامج الذكاء الاصطناعي وتطويرها وتطبيقها قبل فترة طويلة من تفشي COVID-19 في عمليات التشخيص وتطوير بروتوكولات العلاج وتطوير الأدوية، وتقديم العناية والرعاية للمرضى. وتعمل مراكز الأبحاث ومراكز البيانات خلال فترة انتشار وباء كوفيد- 19 على توظيف الذكاء الاصطناعي للبحث عن لقاحات لهذا المرض، وفي هذا السياق تعمل شركة «Deepmind» التابعة لـ «Google» باستخدام نظام (AlphaFold) من خلال تصنيع نماذج لبنية البروتينات المرتبطة بالفيروس سعيا منها لمساعدة الباحثين والعلماء على فهم الفيروس، وتوضح DeepMind على موقعها الالكتروني أن هذه التنبؤات لم يتم التحقق منها تجريبيا[6]، بالإضافة لمحاولات إيجاد مركبات دوائية جديدة، يتم استخدام الذكاء الاصطناعي لإعادة استعمال عدد من الأدوية المعتمدة والمتداولة في أمراض أخرى، وهذا ما من شأنه توفير الوقت والجهد وهو عمل مبني على المحاكاة الحاسوبية[7].

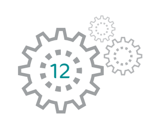
ويجمع الخبراء على أن التوصل إلى علاج فعال للفيروس سيتطلب وقتا طويلا بالإضافة إلى أبحاث وتجارب سريرية عديدة، وفي انتظار ذلك فقد تم اللجوء لاحتياطات احترازية (الحجر الصحي، العزل الاجتماعي، إغلاق الأماكن العامة والمواصلات...) وتمت الاستعانة بتقنيات الذكاء الاصطناعي لمنع تزايد تفشي الوباء وللسيطرة عليه، وهي إجراءات يرى فيها العديد مساسا بالحقوق والحريات الأساسية.

• التتبع

تعمل الحكومات بالتعاون مع شركات الاتصالات وشركات صناعة الأجهزة الذكية في مجموعة من بلدان العالم على تتبع مواقع الأشخاص عبر شبكات الهاتف، وكذا عبر تطبيقات تطلقها على الهواتف والساعات الذكية وأجهزة تتبع اللياقة البدنية، التي تمكن من تحديد مكان المصابين من خلال البيانات الصادرة عنها لتنبه الأشخاص الذين

6. https://deepmind.com/research/open-source/computational-predictions-of-protein-structures-associated-with-COVID-19.

7. عز الدين الابراهيمي، «هذا ما يقوم به الباحثون المغاربة لمواجهة «كورونا»»، مجلة تيليكل، العدد 47، 16-10 أبريل 2020، ص 25.



كانوا بالقرب منهم لفترة معينة من الوقت عبر هواتفهم، كما قامت شركتا Appleو Google بتطوير تطبيقات تستخدم إشارات Bluetooth، ونظام GPS لتحديد المخالطين لحاملي الفيروس وتنبيههم عبر إرسال إشعارات تحذيرية[8].

لقد كانت الصين وكوريا الجنوبية وسنغافورة من أول الدول التي استعانت بتطبيقات التتبع والتعقب بغية السيطرة على انتشار الوباء، وقد لاقت هذه التطبيقات البرمجية رواجا عالميا، فقد أخذت مجموعة من دول العالم الإسلامي بالعمل بها، حيث أطلقت دولة الإمارات العربية المتحدة تطبيق حصن، وفي قطر تطبيق احتراز، وإحمي في تونس، ووقايتنا في المغرب...وفي أوروبا التي تعتبر من أكثر الأماكن تضررا بالفيروس تتسابق الدول لتطوير تطبيقات تساعد على احتواء العدوى، ومنها سويسرا بتطبيق DP-3 T، وفرنسا بتطبيق stopcovid...

مثل هذه التطبيقات من شأنها المساعدة في تقليل مدة الحجر الصحي وما يصاحبه من إجراءات الإغلاق التي أدت لأضرار اقتصادية واجتماعية كبيرة ناهيك عن آثاره النفسية، كما ستساعد السلطاتَ على تحديد خطورة الحالة السريرية للمصابين، ويستعين الأطباء بها كذلك على الفرز بين المرضى الذين في حاجة ماسة إلى عناية سريرية مستعجلة، وبين أولئك الذين بإمكانهم الخضوع للحجر المنزلي، اعتبارا لمحدودية الطاقة الاستيعابية للمستشفيات، واستخدام مثل هذه التطبيقات والأجهزة يمكن أن يساعد المسؤولين في القطاعين الصحي والأمني على اتخاذ القرار والتخطيط الجيد لمواجهة الحالة الوبائية ونتائجها.

- الرقابة

يمكن استعمال تقنيات الذكاء الاصطناعي من قبل السلطات في متابعة مدى التزام الأفراد بإجراءات التباعد الجسدي، وذلك عبر استعمال تطبيقات تعتمد على توظيف بيانات المستخدمين المستقاة من الهواتف المحمولة، وبالتالي رصد تحركاتهم لتحذيرهم حال اقترابهم

8. https://www.bbc.com/arabic/science-and-tech-52250685.

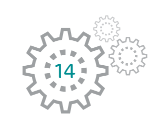


من أماكن تشهد حالات إصابة بالفيروس، وهناك دول أخرى تستعمل الطائرات المسيرة عن بعد والروبوتات في الأماكن العامة لضمان التزام المواطنين بإجراءات التباعد الجسدي، وقد طورت الصين تطبيقات للهواتف الذكية لمراقبة الأشخاص الذين لا يحترمون إجراءات العزل، كذلك عملت روسيا على تطوير شبكة من الكاميرات في الأماكن العامة تتميز بتقنية التعرف على الوجوه لمراقبة مدى احترام تعليمات العزل الاجتماعي.

II. جدوى تطبيقات التتبع الاجتماعي : أسئلة عالقة

إن استخدام آليات الذكاء الاصطناعي في مواجهة فيروس كورونا له إيجابيات عديدة توفر الجهد والوقت وتقلص عدد الضحايا، إلا أن الاستعانة بمجموعة من البيانات ذات الطابع الشخصي عن الحالات المصابة والمخالطين يرى فيها المدافعون عن حقوق الإنسان فكرة مهددة لحريات الإنسان الأساسية، خصوصا فيما يتعلق بالحق في الخصوصية الذي أصبح على المحك بفعل هذه التقنية، حيث أصبحنا نتحدث اليوم عن «نهاية الخصوصية»، في ثنائية جدلية تحاول التوفيق بين مطلب الحرية كحق من حقوق الإنسان الأصيلة والدواعي الأمنية للدول لأجل صون استقرارها وحفظ سلامتها.

لكن الضغط المجتمعي دفع المؤسسات الحكومية لإيجاد حلول ناجعة وسريعة لمواجهة الأزمة الصحية، وامتد هذا الضغط ليشمل المختبرات العلمية والشركات الصناعية التي سارعت لابتكار حلول برمجية وتطبيقات تكنولوجية كفيلة بالاستجابة لهذه التحديات، ولا يخفى مقدار الجاذبية التي تختزنها فكرة توظيف تقنيات الذكاء الاصطناعي في محاصرة الجائحة، وهي بذلك فكرة تغري الشركات والمختبرات لأجل نيل الريادة والكشف عن قدراتها المتقدمة في هذا المجال، لكن لم تُظهر التجارب الحالية لاستخدامات برمجيات التتبع أي فاعلية ملحوظة، فمنفعتها تقتصر على التعرف على الأشخاص القريبين من بؤر الوباء وبالتالي



تسريع وتيرة الكشف عنهم، وهذا أقصى ما يمكن أن تقدمه هذه التقنية إن هي استعملت وفقا للظروف المثالية لاشتغالها، عدا هذا الاستخدام فإن فوائدها تبقى نسبية إلى حد كبيرة وضررها أكبر من نفعها، وقد أكدت العديد من الدراسات إمكانية ظهور تنبيهات زائفة رغم التزام الأفراد بقواعد التباعد الجسدي كاحترام مسافة الأمان والتزام معايير السلامة، ما يجعل من نسبة الإصابة ضئيلة جدا وينزع عن هذه التطبيقات فائدتها، بالإضافة إلى أن استعمال هذه البرمجيات خاضع لإرادة الأشخاص وموافقتهم فقط، دون أن يُنتبه إلى أولئك الذين لا يتوفرون على هواتف ذكية، والذين لا يحسنون التعامل مع البرمجيات المتقدمة خصوصا من الفقراء وكبار السن[9] ...

حتى في الحالات الأكثر عرضة للتقارب الجسدي بين الأفراد، فإن نسبة العدوى تبقى ضئيلة حيث لا يتعدى عدد المخالطين معدل عشرات الأشخاص يوميا، أما في الحالات العادية وفي غياب شروط التباعد التجسدي فإن متوسط الإصابة هو من شخصين إلى ثلاث أشخاص[10]، بذلك فإن قيام هذه البرمجيات بإرسال تنبيهات في حالة التواصل اليومي العابر بين الأشخاص والذي تكون فيه نسبه العدوى ضئيلة جدا من شأنه أن يوسع دائرة التنبيه دون فائدة، وإن تمت الاستجابة لهذه التنبيهات الزائفة فسوف يُضطر المستخدمون إلى الاستجابة لها، ما سيجبرهم على الدخول في حجر صحي طوعي رغم عدم إصابتهم، ثم إن المستخدمين عند إدراكهم لكيفية اشتغال هذه البرمجيات بالشكل الذي أشرنا له سابقا، سيجعلهم يعتادون على تجاهل التنبيهات المتوصل بها، مما سينزع عن هذه البرامج فائدتها.

لكن التساؤل يثور حول مدى دقة هذه البرامج وجدواها، فماذا يمكن أن يحدث إن تمت مشاركة بيانات مغلوطة ناتجة عن تشخيص غير مضبوط أو لعطب أصاب التطبيق البرمجي ؟ ما سيترتب عنه إرسال إنذارات

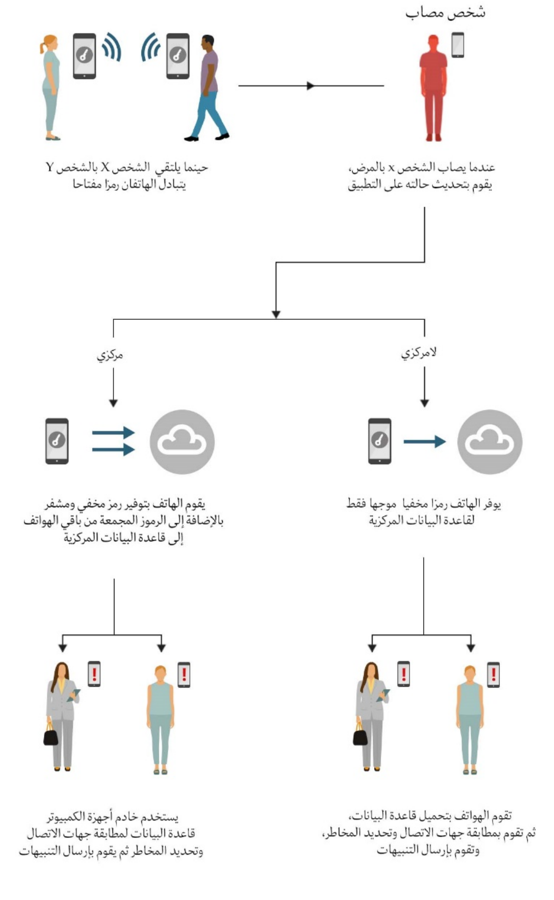
9. https://www.nytimes.com/2020/04/23/world/europe/coronavirus-R0-explainer.html.

10. https://www.nytimes.com/2020/04/23/world/europe/coronavirus-R0-explainer.html.



زائفة متعلقة بشخص ما على نطاق واسع غير متحكم فيه واعتباره ضمن دائرة المصابين وهو ليس كذلك، كيف يمكن تدارك هذا الخطأ خصوصا عندما سيضطر الناس بفعل هذا الإنذار الخاطئ إلى الحجر على أنفسهم تلقائيا[11] ؟

ماذا عن الأشخاص الذين يعانون الهشاشة الاجتماعية والفقر ولا يملكون هاتفا ؟ وهل يحمل الناس هواتفهم معهم في كل تحركاتهم؟ حتى في بلد مصنع للهواتف المحمولة بتغطية شبكية متطورة مثل الولايات المتحدة فإن نسبة الذين يمتلكون هاتفا محمولا هي 81 في المئة[12]، ماذا لو ترك أحدهم هاتفه في السيارة



https://www.bbc.com/news/technology-52355028

أو في مكان ما؟ بل إن الهاتف نفسه سيصبح أداة لنقل العدوى ما دام الفايروس ينتشر فوق سطح أي شيئ مادي[13]، في هذه الحالة فإن أكثر الأشخاص عرضة للعدوى هم كبار السن الذين غالبا لا يتقنون التعامل

11. https://www.nature.com/articles/d41586-020-01264-1.
12. https://www.pewresearch.org/internet/fact-sheet/mobile/.
13. https://www.nih.gov/news-events/news-releases/new-coronavirus-stable-hours-surfaces.



مع مثل هذه البرمجيات وكذلك الأشخاص الذين في وضعية اجتماعية هشة، فكيف يمكن تمكين هؤلاء من الولوج إلى مثل هذه البرمجيات ؟ وفي حالة ما إذا تأكد صاحب الهاتف من مخالطته لشخص مصاب، فهل سيصرح بنفسه كمصاب ضمن قاعدة بيانات المصابين ؟ أم قد يعتريه الخوف الاجتماعي من نظرة الناس إليه وبالتالي قد يُفَضِّلُ إخفاء حالته المرضية خصوصا إذا لم تظهر عليه أعراض الوباء.

إن برامج التتبع الفردي ليست بضمانة كافية لتأمين تنقل الناس، فخلو المناطق المجاورة والمحيطة بالمستخدِم ليس بالأمر الذي سيحمي الناس من الوباء، وهذه التطبيقات في أصلها إجراء يستهدف الصحة العامة لا الصحة الفردية، أي أنها تساعد في التقليل من انتشار المرض على صعيد المواطنين كافة، لكنها لا تمنح الحماية الصحية لأي فرد بذاته، ما يولد مشاكل أخرى بحاجة إلى مزيد من التفكير، ماذا سيحدث إن صدّق الناس هذه التنبيهات الزائفة فتجنبوا الاجتماع البشري ودخلوا في حجرذاتي وطوعي، وما تبعات ذلك على عملهم وعلى الحالة الاقتصادية للدول ككل ؟

لا ننفي هنا وجود بعض البرمجيات التي راعت في تصميمها واشتغالها مسألة الأمن الشخصي وحماية المعطيات الشخصية، مثال ذلك البرنامج التي وضعته غووغل بالتعاون مع برنامج آبل لهذا الغرض، حيث يقوم هذا التطبيق بتخزين المعلومات حول الأجهزة المتصلة فيما بينها دون تحويل هذه المعلومات إلى خادم (Server) مركزي كما هو الحال في التطبيقات الأخرى، لكن حتى هذه الفكرة لا تخلو من تهديدات لخصوصية الأشخاص وأمنهم، لأن تشغيل هذه التطبيقات انطلاقا من واجهة برمجة التطبيقات (Application programming interface (API)) سيفتح الباب لثغرات أمنية جديدة تستهدف الخصوصية الشخصية، مثال ذلك إظهار تطبيقات تتبع المتصلين للحالة الصحية لمستخدم ما عبر إمكانية ربط الأشخاص المصابين بصورهم عبر كاميرا ثابتة متصلة بجهاز Bluetooth في الأماكن العامة[14].

14. https://www.wired.com/story/apple-google-contact-tracing-strengths-weaknesses/.



وباستحضار المناخ العام الحالي المشحون بالأخبار الزائفة التي تعج بها بعض مواقع التواصل الاجتماعي والمنابر الإعلامية، فإن التوظيف المشبوه لمثل هذه المعطيات وارد جدا خصوصا في الدعاية الزائفة وفي الاستعمالات الكيدية والتضييق على المنافسة الاقتصادية الحرة، فقد يحدث أن يُبَلِّغَ شخص عن إصابة شخص آخر لغرض انتقامي مثلا، ماذا سيحدث إن وقع خطأ ما في عملية رصد الوباء على مستوى مدينة بأكملها وتقرر الحجر عليها بالكامل واعتبارها بؤرة وبائية ؟ هنا تظهر لنا مكامن الضعف والتهديد في هذه البرمجيات والمنصات التي لم يتطرق الحقوقيون لها بعد وكذلك المهتمون بالجوانب الأخلاقية لهذه التقنية، رغم أن مصممي هذه البرمجيات يعترفون بصفة عامة في وثائقهم بإمكانية توظيف هذه البرمجيات لأغراض غير حميدة ومشبوهة، غير أن لابد لهذه الشركات من التزام النزاهة والصدق في تحديد هذه الثغرات البرمجية ومحدودية هذه التكنولوجيا، إضافة إلى أن هذه التقنيات لا ينبغي أن توظف منفردة، بل ينبغي إرفاق هذه البرمجيات بكل التوضيحات المتعلقة بها كما هو الحال في العديد من السلع والبضائع التي يتم الإشارة فيها إلى أمد حياة المنتج ونقاط ضعفه والمنهيات الواجب تجنبها عند الاستخدام.

وقد حدث في العديد من الدول أن طالب أصحاب المحلات من الزبائن إظهار هواتفهم للتأكد من خلوهم من الوباء كشرط للولوج، ويزداد التخوف من أن يتحول الطابع الاختياري في استخدام هذه التطبيقات إلى طابع إلزامي وشرطي لأجل أي تفاعل اجتماعي يومي للأفراد، سواء من لدن صناع السياسات والتجار والمستخدمين والسياح وفي كل مناحي الخدمات العامة[15]، ما سوف يزيد من حدة النبذ والإقصاء الاجتماعي، والمنع من ولوج الأماكن العامة والخاصة و تقليل المشاركة في الأنشطة الاجتماعية والاقتصادية، خصوصا لدى الأشخاص الذين يُعلن عن إصابتهم وكذلك أقربائهم حيث سيصبحون أكبر المتضررين

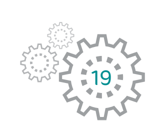
15. https://www.hawaiinewsnow.com/2020/04/24/welcome-hawaii-heres-your-ankle-monitor-stronger-policies-track-tourists-eyed/.



من هذا الاقصاء الاجتماعي، أما في الأوساط المكتظة بالسكان كما هو الحال في المدن الضخمة وفي الدول ذات الدخل المنخفض، فإن حالات التبليغ الزائف عن الإصابات ترتفع نظرا للتخوف الذي يولده القرب الشديد بين السكان والعائلات والأفراد.

تبعا لهذا فإن الشركات المصممة لتطبيقات التتبع مدعوة إلى توخي الصدق والوضوح في إبراز محدودية هذه التقنيات، وتوفير دلائل إرشادية حول الممارسات السليمة والمثلى والتوصيات والنصائح المتعلقة بهذه التطبيقات والعمليات الخلفية التي تتم وراء واجهات التطبيقات من أجل تأمين بيانات المستخدمين، والكشف عن مدة الإبقاء على هذه البيانات، ثم بسط المحددات المعتمدة في تجميع معلومات المواطنين من لدن المؤسسات الصحية العامة مثل الموقع الجغرافي وبيانات الهوية الشخصية، وينبغي كذلك الاتفاق على أنظمة تدقيق أمني مشتركة بين الحكومات والشركات المصمّمة، والإعلان عن تحفيزات ومكافآت مخصصة لمكتشفي أي ثغرة أمنية أو إضرار أو تعسف أو أذى قد يمس المستخدمين، وفي الأخير فإن الشركات والمؤسسات المصممة لهذه البرمجيات ينبغي أن تتعهد بأجل محدد ينتهي عنده الاشتغال بهذه التطبيقات المؤقتة ويستغنى عنها.

وهنا يبرز دور التنظيم القانوني والسياسات الحكومية في وضع السبل الكفيلة بحماية الأفراد من تعسف التقنية، وعلى رأسها مؤسسات العدالة عبر الرقابة القضائية ضد أي توسيع أو شطط في استعمال هذه التطبيقات وضد إي إبقاء على البيانات الشخصية للمستخدمين بعد انقضاء أجل العمل بها، لأجل الغاية المثلى المتمثلة في صيانة الحقوق وحفظ الحريات ودفع أي انحراف من شأنه تهديد حياة الناس وأمنهم، ولهذا فعلى القانونيين ومنظمات المجتمع المدني المعنية بالدفاع عن حريات الأفراد وحقوقهم أن يتفاعلوا ويأخذوا بزمام المبادرة في التنبيه إلى أي خرق أو انتهاك وفق نهج استباقي، حتى لا يترتب عن تجميع هذه البيانات الشخصية للأفراد أي تمييز أو إقصاء



اقتصادي أو اجتماعي بسبب التطبيقات البرمجية ونظم المعلومات المصممة لمواجهة الوباء، وقد قامت مجموعة من الأكاديميين في المملكة المتحدة باقتراح نموذج تشريعي رائد ومتقدم يستهدف منع أي استخدام جبري أو إلزامي لهذه التطبيقات التي لم تُختبَر بعد حتى لا تكون مانعا أمام الأفراد من أن يلجوا المرافق العامة ويستفيدوا من خدماتها[16]، ولهذا فإن تكنلوجيا الذكاء الاصطناعي بحسناتها العديدة غير قادرة، لوحدها، على مجابهة هذا الوضع الصحي الحالي الحرج، لكن الحرص ينبغي أن ينصب على دفع أي إضرارمن شأن هذه التقنية أن تشكله على الناس.

16. https://osf.io/preprints/lawarxiv/yc6xu/.



المحور الثاني : الأطر القانونية الدولية لحماية الخصوصية

ترتكز مختلف التقنيات المعتمدة في مكافحة فيروس كورونا المُتبعة من قبل حكومات بعض الدول أساسا على قاعدة بيانات ضخمة حول المواطنين في أنحاء البلاد، تتضمن أسماءهم ومناطق إقامتهم وأماكن عملهم حتى يسهل رصد حركاتهم وحالتهم الصحية[17]، ولعل السرعة في الوصول إلى هذه البيانات راجعة لما للذكاء الاصطناعي من قدرة على حفظ كمية هائلة من البيانات وتداولها بسرعة ليس فقط ضمن إطار دولة واحدة، وإنما على مستوى دول العالم قاطبة بما في ذلك البيانات الخاصة بالأفراد، مثل (الإسم، الأصل، العنوان، الآراء والمعتقدات، التفاصيل الطبية...).

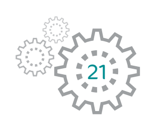
وبالرغم من أهمية الإجراءات في الحد من انتشار الفيروس فإن معالجة وتحليل هذه البيانات الشخصية وغيرها من شأنه تعريض الخصوصية الفردية للتهديد والانتهاك، نظرا لأن هذه البيانات لا يقتصر الولوج إليها على أجهزة الدولة فقط ولكنها معرضة للاختراق من قبل الأشخاص أيضا، مما يسهل إمكانية انتهاك الحياة الخاصة للأفراد، وبالتالي المساس بأهم حق من الحقوق الإنسانية المنصوص عليها في المواثيق الدولية والتشريعات الوطنية للدول.

I. حماية الخصوصية من خلال المواثيق الدولية والإقليمية

برز الحق في الخصوصية[18] قبل عصر انتشار النظم الصناعية من خلال حق الفرد في حماية البيئة الخاصة به، إلا أنه في ظل تطور الذكاء الاصطناعي وسهولة انتهاك هذا الحق، أصبحت حماية الخصوصية

17. الموقع الالكتروني www. al-ain.com.

18. إن مفهوم الخصوصية يتغير من بلد لآخر، ويمكن القول بأن الخصوصية هي رسم الحدود التي تنظم قدرة المجتمع على التدخل في حياة الفرد عبر حماية بعض بياناته الشخصية، بشكل يمنع انتشار المعلومات المتعلقة به، وعليه هناك اعتداء على الخصوصية سواء تعلق الأمر بكشف أسرار خاصة أو بنشر معلومات أو ترصد تحركات الفرد.



ضرورة ملحة سواء من خلال الاتفاقيات الدولية أو الإقليمية، واختلفت التعريفات بشأن تحديد مفهوم محدد للخصوصية غير أنها تلتقي كلها على الحق في الحياة الخاصة[19]، ويزيد آخرون بأنها قدرة الشخص على حفظ أموره الشخصية ومنع انتهاكها، ومفهوم الخصوصية هو مفهوم قديم قدم الإنسان بحيث اختلفت تمثلاته باختلاف الثقافات والحضارات، فنجد في الفقه الإسلامي التنصيص على مفهوم «الحرمات» الذي يشير إلى وجوب حفظ النفس والعرض والمال، ونجد في الفقه الفرنسي مفهوم الخصوصية يشير إلى كل ما يتعلق بالحياة الخاصة كالعلاقة بالأبناء والزوجة والعائلة والصورة والذمة المالية والخلوات وغيرها[20]...، غير أن الثورة الرقمية أوجبت مزيدا من الحماية لهذا الحق بفعل اختراقها لكل مجالات الحياة العامة والخاصة[21].

1. الإعلان العالمي لحقوق الإنسان والعهد الدولي للحقوق المدنية والسياسية

ورد في المادة 12 من الإعلان العالمي لحقوق الإنسان لسنة 1948 ما يلي : «لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمس شرفه وسمعته، ولكل شخص الحق في أن يحميه القانون من مثل ذلك التدخل أو تلك الحملات»، كما نص العهد الدولي للحقوق المدنية والسياسية لسنة 1966 من خلال مادته 17 على أنه : «لا يجوز تعريض أي شخص على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته، أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته، من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس».

19. علي أحمد عبد الزعبي، حق الخصوصية في القانون الجنائي، المؤسسة الحديثة للكتاب، لبنان، 2006، ص 32.

20. حسام الدين الاهواني، الحق في احترام الحياة الخاصة، دراسة مقارنة، دار النهضة العربية، 1978، ص 23.

21. التقرير السنوي لمفوضية الأمم المتحدة السامية لحقوق الانسان وتقارير المفوضية والأمين العام، الحق في الخصوصية في العصر الرقمي، مجلس حقوق الانسان، الدورة السابعة والعشرون، A/HRC/27/37، 30-June- 2014.



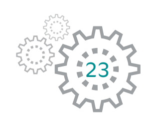
وأكد كل من الإعلان العالمي لحقوق الإنسان والعهد الدولي للحقوق المدنية والسياسية على الحماية القانونية للخصوصية، وقد علقت اللجنة الدولية لحقوق الإنسان التابعة للأمم المتحدة على المادة 17 من العهد الدولي للحقوق المدنية والسياسية على أن الحق في الخصوصية يشمل الحق في الحماية «ضد كل تلك التدخلات والاعتداءات سواء كانت صادرة عن سلطات الدولة، أو من الأشخاص الطبيعيين والاعتباريين» ولكن التوسع في تحديد أسباب الاعتداء يفتح المجال أمام الاعتداءات الناتجة عن توظيف الذكاء الاصطناعي في خرق الخصوصية خاصة في مجال رصد التحركات والحالة الصحية للأفراد عن طريق جمع ومعالجة هذه المعطيات الشخصية والتي تعتبر جزءا من الخصوصية، وفي هذا الإطار جاء التعليق العام رقم 16 للجنة الدولية لحقوق الإنسان ليؤكد على مكانة المعطيات الشخصية في الخصوصية، حيث أعطت الحق للأفراد في التأكد من المعلومات التي يحتفظ بها عنهم وأغراض حفظها والجهة التي تحتفظ بها[22].

2. التقرير الصادر عن المفوض السامي في مجلس حقوق الانسان

واعتمدت الجمعية العامة للأمم المتحدة القرار 68/ 167 في كانون الأول/ديسمبر 2013، [23] الذي أعربت فيه عن القلق البالغ إزاء الأثر السلبي الذي يمكن أن تخلفه مراقبة الاتصالات واعتراضها على حقوق الإنسان، وأكدت الجمعية العامة أن حقوق الأشخاص خارج الفضاء الإلكتروني يجب أن تحظى بالحماية أيضاً في الفضاء الإلكتروني، وأهابت بجميع الدول أن تحترم وتحمي الحق في الخصوصية في الاتصالات الرقمية، وأهابت الجمعية العامة بجميع الدول أن تعيد النظر في إجراءاتها وممارساتها وتشريعاتها المتعلقة بمراقبة الاتصالات

22. تنص المادة 17 (الحق في حرمة الحياة الخاصة) من التعليق العام رقم 16 الصادر عن اللجنة الدولية لحقوق الإنسان سنة 1988، على حق كل شخص في عدم التعرض، - على نحو تعسفي أو غير مشروع - لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته ولا لأي حملات لا قانونية تمس بشرفه أو سمعته، وترى اللجنة أنه يلزم ضمان هذا الحق في مواجهة جميع تلك التدخلات والاعتداءات سواء أكانت صادرة عن سلطات الدولة أم عن أشخاص طبيعيين أو قانونيين، المادة 17 الحق في حرمة الحياة الخاصة. www.hrlibrary.umn.edu.


23. http://undocs.org/A/RES/68/167.



واعتراضها وجمع البيانات الشخصية، وشددت على ضرورة أن تضمن الدول تنفيذ التزاماتها بموجب القانون الدولي لحقوق الإنسان تنفيذاً كاملاً وفعالاً[24]. من خلال اعتماد القرار 68/167، طلبت الجمعية العامة من المفوضة السامية لحقوق الإنسان إعداد تقرير عن الحق في الخصوصية في العصر الرقمي، ويتعين أن يتناول التقرير بالبحث، وفقاً لنص القرار : «حماية الحق في الخصوصية وتعزيزه في سياق المراقبة الداخلية والخارجية للاتصالات الرقمية و/أو اعتراضها وجمع البيانات الشخصية، بما في ذلك على نطاق جماعي»، ولإعداد هذا التقرير فقد اضطلعت المفوضية السامية لحقوق الإنسان بأعمال بحث وتشاور مع مختلف الجهات المعنية، واتصلت بالشركاء داخل منظومة الأمم المتحدة وخارجها، وشجعت المفوضية جميع الأطراف المهتمة على تبادل المعلومات ووجهات النظر بشأن المسائل المثارة في القرار 68/167.

ووفقاً لما يشير إليه القرار 68/167، فإن القانون الدولي لحقوق الإنسان يوفر الإطار العالمي الذي يجب أن يُقيَّم على أساسه أي تدخل في حقوق الخصوصية الفردية وينص العهد الدولي الخاص بالحقوق المدنية والسياسية الذي صدّقت عليه حتى الآن 167 دولة، على أنه لا يجوز تعريض أي شخص على نحو تعسفي أو غير قانوني للتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته، وينص العهد بالإضافة إلى ذلك، على أن «من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس».

وتتضمن صكوك دولية أخرى لحقوق الإنسان أحكاماً مماثلة، في حين أن الحق في الخصوصية بموجب القانون الدولي ليس حقاً مطلقاً، فإن أي حالة تدخل يجب أن تخضع لتقييم دقيق ونقدي لمدى ضرورتها ومشروعيتها وتناسبها.

24. انظر المذكرة الشفوية الموجهة للدول الأعضاء https://www.ohchr.org/Documents/Issues/Privacy/NV.pdf.

نفس المقتضى نصت عليه المادة 11 من الاتفاقية الأمريكية حيث ورد فيها : «لكل إنسان الحق في أن يحترم شرفه وتصان كرامته ولا يجوز أن يعترض أحد لتدخل اعتباطي أو تعسفي في حياته الخاصة أو شؤون أسرته أو منزله أو مراسلاته، ولا أن يعترض لاعتداءات غير مشروعة على شرفه أو سمعته، ولكل إنسان الحق في أن يحميه القانون من مثل ذلك التدخل أو تلك الاعتداءات[25]»، وقد نصت المادة الرابعة من الميثاق الإفريقي لحقوق الإنسان والشعوب على ما يلي : «لا يجوز انتهاك حرمة الإنسان، ومن حقه احترام حياته وسلامة شخصه البدنية والمعنوية، ولا يجوز حرمانه من هذا الحق تعسفا[26]».

3. الاتفاقية الأوروبية لحقوق الإنسان

كما نصت المادة الثامنة من الاتفاقية الأوروبية لحقوق الإنسان على ما يلي : «لكل إنسان حق احترام حياته الخاصة والعائلية ومسكنه ومراسلاته، و لا يجوز للسلطة العامة أن تتعرض لممارسة هذا الحق إلا وفقا للقانون وبما تمليه الضرورة في مجتمع ديمقراطي لصالح الأمن القومي وسلامة الجمهور أو الرخاء الاقتصادي للمجتمع، أو حفظ النظام ومنع الجريمة أو حماية الصحة العامة والآداب، أو حماية حقوق الآخرين وحرياتهم[27]» .

4. منظمة التعاون والتنمية الاقتصادية[28]

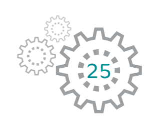
أصدرت منظمة التعاون والتنمية الاقتصادية بتاريخ 23 سبتمبر 1980 توصيات تتعلق بالمبادئ التوجيهية بشأن حماية الحياة الخاصة ونقل

25. الاتفاقية الأمريكية لحقوق الإنسان المصادق عليها بسان خوسيه، بتاريخ 22 نونبر 1969.

26. الميثاق الإفريقي لحقوق الإنسان والشعوب المصادق عليه بنيروبي في يونيو 1981.

27. اتفاقية حماية حقوق الإنسان في نطاق مجلس أوروبا المصادق عليها بروما بتاريخ 4 نونبر 1950.

28. منظمة التعاون والتنمية الاقتصادية Organisation de coopération et de développement économiques : أنشئت في 30 سبتمبر 1961 بعد أن حلت محل منظمة التعاون الاقتصادي الأوربي، تتضمن مجموعة من البلدان المتقدمة التي تقبل مبادئ الديموقراطية التمثيلية واقتصاد السوق الحر، تم توسيعها لتشمل في عضويتها بلدان غير أوروبية كالولايات المتحدة الأمريكية، واليابان، وكوريا الجنوبية، والتشيلي وغيرها من الدول غير الأوروبية، وهو ما يضفي على هذه المنظمة الصفة العالمية وعلى الاتفاقيات والتوجهات الصادرة عنها.



وتدفق البيانات المعالجة آليا أو غير آليا، وتطبق على القطاع العام والخاص، تتضمن هذه التوصيات المبادئ التالية :

1. محدودية عمليات جمع البيانات
2. نوعية البيانات
3. تحديد الغرض
4. حصر الاستخدام بالهدف المحدد
5. تأمين وسائل حماية وأمن المعلومات
6. العلانية
7. الحق في المساءلة والمشاركة

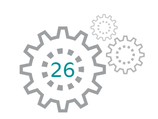
ورغم كون التوصيات الصادرة عن منظمة التعاون والتنمية الاقتصادية غير ملزمة تجاه الأعضاء، إلا أنها كانت الموجه الأساسي لتشريعات الدول الأوروبية[29].

5. الاتفاقية 108 لمجلس أوروبا

تضمنت الاتفاقية رقم 108 المتعلقة بحماية الأشخاص الذاتيين تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي، الموقعة بستراسبورغ في 28 يناير 1981، مجموعة من المبادئ الأساسية الخاصة بحماية المعطيات أهمها التزام كل دولة طرف بالتنصيص في قوانينها الداخلية على التدابير الضرورية لحماية المعطيات ذات الطابع الشخصي سواء من الناحية الموضوعية أو الإجرائية، وإدراج التدابير الأمنية ضمن قوانينها، حماية للهوية والحقوق والحريات الفردية والجماعية والحياة الخاصة من كل ما من شأنه أن يمس بها عبر استخدام المعلومات.

كما تضمنت الاتفاقية وجوب احترام الحقوق والحريات الأساسية لجميع الأشخاص الذاتيين المتواجدين على إقليم كل دولة طرف فيها، بغض

29. مقال منشور بموقع www.sitcegypt.org تحت عنوان الحماية القانونية للبيانات الشخصية.



النظر عن جنسيتهم أو إقامتهم، خاصة حقهم في الحياة الخاصة تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي.

وأكدت على ضرورة تقوية أوجه التعاون الدولي للقضاء على الجرائم المعلوماتية حيث من شأن تضامن أطراف هذه الاتفاقية محاربة هذا النوع من الجرائم، وبالتالي حماية الأشخاص الذاتيين تجاه معالجي المعطيات ذات الطابع الشخصي[30].

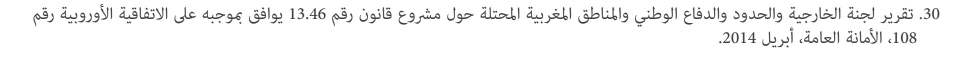
وبالنظر إلى التطور الرقمي وما يخلفه من تبادل البيانات عبر الحدود الدولية، كان لا بد من تعديل هذه الاتفاقية عن طريق توقيع برتوكول إضافي بتاريخ 8 نونبر 2001 تم التركيز فيه على ما يلي :

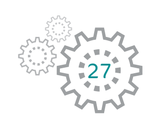
- تأسيس لجان متخصصة لمراقبة حسن تطبيق الاتفاقية الأصلية الصادرة سنة 1981.
- تدفق البيانات عبر الحدود بشرط أن تكون الدولة المرسل إليها متمتعة بمستوى مماثل من الحماية المقررة.

ويعتبر البرتوكول الصادر سنة 2018 آخر برتوكول تعديلي للمعاهدة حتى الآن والذي تضمن تكييف مبادئ حماية البيانات الخاصة بها مع الأدوات الجديدة والممارسات الجديدة.

6. المنظمة العالمية للتجارة

جاء في الفصل 14 من الاتفاقية المؤرخة في 15 أبريل 1994 المحدثة للمنظمة العالمية للتجارة ما يلي : «تحت التحفظ على ألا تكون هذه الضوابط مطبقة بشكل يؤدي إلى اعتبارها وسيلة للتمييز التحكمي أو غير المبرر بين الدول التي توجد فيها ظروف مماثلة، وإلى أي تقليص بدعوى أن الأمر يتعلق بتجارة الخدمات، فإن كل مقتضى


30. تقرير لجنة الخارجية والحدود والدفاع الوطني والمناطق المغربية المحتلة حول مشروع قانون رقم 13.46 يوافق بموجبه على الاتفاقية الأوروبية رقم 108، الأمانة العامة، أبريل 2014.



من هذه الاتفاقية لا يمكن تأويله على أنه يمنع أي دولة عضو من تبني أو تطبيق الإجراءات الضرورية لضمان احترام القوانين والأنظمة التي لا تتعارض معها، ومن ضمنها تلك المتعلقة بحماية الحياة الخاصة للأشخاص تجاه معالجة ونشر المعطيات الشخصية، وبحماية الطابع السري للملفات والحسابات الشخصية[31]».

إن المنظمة العالمية للتجارة ومن خلال الاتفاقية السابقة أكدت هي الأخرى على ضرورة حماية حقوق وحريات الأشخاص عالميا، على اعتبار أن تبادل المعطيات الشخصية بفضل التطور الحاصل في التجارة الالكترونية لا يبرر الاعتداء على الخصوصية.

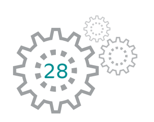
7. الاتحاد الأوروبي

يمتلك الاتحاد الأوروبي سياسة واضحة فيما يتعلق بحماية بيانات المواطنين الأوروبيين تجاه الشركات التي تُجَمِّع أو تستطيع الوصول إلى البيانات الشخصية، حيث دخل النظام الأوروبي العام لحماية البيانات General Data Protection Regulation حيز التنفيذ في 25 ماي 2018، واختص بحماية البيانات والخصوصية لجميع الأفراد داخل الاتحاد الأوروبي، ويتعلق أيضا بتصدير البيانات الشخصية خارج الاتحاد الأوروبي، وهو يهدف لمنح المواطنين القدرة على التحكم والسيطرة بالبيانات الشخصية وتبسيط بيئة التنظيمات، حيث يضمن للشخص جملة من الحقوق تشمل الحق في معرفة البيانات التي تمتلكها الشركات عنه، وحقه في النسيان (حذف سجله كاملا دون عودة)[32]، ويرتب على الشركات غرامات مالية ضخمة في حال عدم التزامها.

إن كل هذه الترسانات القانونية المنصوص عليها في المواثيق الدولية لم تثن بعض الدول (ألمانيا، سنغافورة) من استعمال تطبيقات خاصة على الهواتف الذكية بعد رفع الحجر الصحي من أجل استمرار تتبع فيروس

31. ACCORD INSTTUANT L'ORGANISATION MONDIALE DU COMMERCE ,www.tfig.unece.org.

32. www.europarabct.com.



كورونا لمنع أي موجة ثانية من الجائحة، يبقى النقاش قائما حول من الأولى بالحماية ؟ هل الحق في الخصوصية أم الحق في الحياة ؟

بالرغم من أن الحَقَّيْن معا هما من صميم الحقوق الأساسية للإنسان في التشريعات العالمية إلا أنه لا يمكن الجزم لحد الآن بكون هذه التطبيقات التي تعتمد التتبع عن طريق استخدام البيانات الخاصة بموقع الهاتف الذكي للشخص، وفي حالة ثبوت إصابة صاحب الهاتف بالفيروس يتم تنزيل هذه البيانات أفرِقة التتبع للتواصل سريعا مع الأشخاص المحيطين والمعرضين للإصابة المحتملة بالمرض، ما يعني إمكانية جعل كل الخصوصية الفردية ومبدأ الحماية الشخصية التي تم التفصيل فيها سابقا على المحك، خاصة وأن دول آسيا اعتمدت هذه التطبيقات بشكل لا يمكن لمستخدمي الهواتف الذكية من الإفلات منه، حيث لا بد من مسح الرمز الشريطي QR بواسطة الهاتف المحمول قبل الدخول إلى أي مبنى، فيتم استخدام بياناتهم دون موافقتهم حيث أن المعلومات المتعلقة بالاتصالات في قاعدة البيانات تدار من طرف الحكومة.

هذا الأمر جعل دولا مثل ألمانيا تطور تطبيق التتبع لجعله أقل تدخلا في الخصوصية، كما جعلت تنزيله على أساس طوعي، وفرضت احترام هذا التطبيق لقانون حماية البيانات الألماني، ونفس التطبيق DP-3T اعتمدته سويسرا بتاريخ 5 ماي، 2020 وقد عرف هذا التطبيق معارضة من الخبراء القانونيين السويسريين على اعتبار أن جميع الدول التي استخدمت هذه التطبيقات لم تثبت فعاليته في الحد من انتشار الفيروس، كما أن استخدام مثل هذه التطبيقات لا يضمن عدم التعرض للاختراق، مما يؤدي إلى تعريض خصوصيات الأشخاص للخطر خاصة وأن من شأن الموافقة على اعتماد أنظمة للمراقبة وقت الأزمات قد يجعلها أمرا دائما وليس مؤقتا[33].

33. https//:www.Swissinfo.ch “Coronavirus contact tracing app friend or foe?”.



بالرغم من تطوير هذه التطبيقات لتحترم خصوصيات الأفراد فإن التجربة وحدها الكفيلة بحسم هذا الجدل، فإذا ما تم ثبوت خرقها لنظام المعطيات الشخصية فسوف يتم تطبيق المقتضيات المنصوص عليها في المواثيق الدولية السابق ذكرها، إذ لا يمكن التغاضي عن هذه الانتهاكات بدعوى حماية الحق في الحياة، وهو ما اعتمده قاضي الأمور المستعجلة بمجلس الدولة الفرنسي من خلال قراره[34] الصادر في 18 ماي 2020 تحت عدد 440442، 440445.

فبالرغم من كون اعتماد الطائرة بدون طيار Drone ساهم في الحد من انتشار الفيروس عبر تتبع المخالفين لإجراءات الحجر الصحي وتعقب حركة الأشخاص إلا أنها تشكل خرقا للخصوصية، مما جعل مجلس الدولة الفرنسي يوقف استخدامها ويرتب غرامة على استعمالها من قبل الدولة.

II. حماية حماية الخصوصية من خلال قوانين بعض الدول الأعضاء في منظمة الإيسيسكو

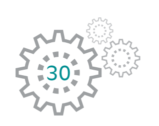
في ظل الاجتياح العالمي لفيروس كورونا، فإن الدول الأعضاء في منظمة الإيسيسكو، كباقي الدول التي عرفت انتشارا للوباء، وظفت تقنيات الذكاء الاصطناعي للحد من انتشاره، واتخذت تقنيات التتبع والتشخيص عن طريق التطبيقات الإلكترونية المعمول بها الدول الغربية أو عن طريق استخدام تقنيات خاصة بها، ما يطرح التساؤل حول مدى حماية حق الخصوصية من خلال قوانينها الوطنية، والإجراءات والوسائل التي نهجتها لاحتواء الوباء، ونتطرق هنا إلى بعض التجارب المتقدمة

34. المادة 1 : يلغي أمر قاضي الأمور المستعجلة بالمحكمة الإدارية في باريس الصادر بتاريخ 5 ماي 2020.

المادة 2 : وفقا لأسباب هذا الأمر، تلزم الدولة بأن توقف، ودون أجل، تنفيذ تدابير مراقبة احترام قواعد الأمن الصحي السارية على فترة رفع الحجر الصحي في باريس بطائرة بدون طيار.

المادة 3 : تدفع الدولة لجمعية «La quardrature du net» «ورابطة حقوق الإنسان» مبلغ 3000 يورو لكل منهما بموجب المادة L 1-761. من قانون القضاء الإداري.

المادة 4 : يبلغ هذا الأمر لجمعية «La quardrature du net» «ورابطة حقوق الإنسان ووزير الداخلية».



من دول العالم الإسلامي في محاولة لتقييم عمل النظم القانونية والهيئات الرقابية المعهود إليها بحماية خصوصية البيانات الشخصية من خلال تشريعاتها الوطنية و من خلال تطبيقات برامج الذكاء الاصطناعي المخصصة لمواجهة الوباء.

1. القانون الجديد لحماية البيانات الشخصية في أندونيسيا

تُعدّ إندونيسيا من أهم الاقتصادات الرقمية التي تشهد نموا متسارعا جدا في منطقة آسيا والمحيط الهادئ[35]، وينص الدستور الإندونيسي على الحق في الخصوصية، ولم تكن الجمهورية الإندونيسية تمتلك قانونا مستقلا يحمي البيانات الخاصة، غير أننا نجد مقتضيات تنص على حماية البيانات الخاصة في قانون المعلومات والمعاملات الإلكترونية[36] (EITL) الذي جرى تتميمه بالقرار الحكومي رقم 71 سنة 2019 المتعلق بأحكام النظم والمعلومات الإلكترونية[37]، ثم تُمّم بالقرار الوزاري رقم 20 لوزير الاتصالات والمعلوماتية والمتعلق بحماية البيانات الشخصية في الأنظمة الإلكترونية[38].

وقام رئيس جمهورية إندونيسيا بتوقيع مسودة قانون حماية البيانات الشخصية (PDP Draft Law) في يناير 2020، وتمت مناقشة المسودة في مجلس النواب، ويُنتظر أن يُنشر ويُوافَق عليه في نهاية هذه السنة، ويشكل هذا القانون إطارا جديدا تمت صياغته سيرا على النظام الأوروبي العام لحماية البيانات، وسوف يَنسَخ هذا القانون الجديد كل المقتضيات السابقة، كما يستهدف في تنظيمه القطاعين العام والخاص، ويعزز السيادة والحماية المعلوماتية وينظم البيانات الخاصة والحساسة للأشخاص ويُحسِّن من جودتها ودقتها وتدفقاتها عبر الحدود.

35. https://www.reuters.com/article/us-indonesia-data/indonesia-to-step-up-data-protection-with-new-bill-amid-booming-digital-economy-idUSKBN1ZR1NL
36. http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4846_UU_11_2008_e.html.
37. https://www.bakermckenzie.com/en/insight/publications/2019/10/new-regulation-electronic-system-and-transactions.
38. http://makna.co/wp-content/uploads/2018/01/MOCI-Regulation-No-20-of-2016-Makna-Eng.pdf.



وينص القانون الجديد على قاعدة «الرضا» كأساس لمعالجة البيانات الخاصة ما لم ينص قانون آخر على خلاف ذلك، والمقصود بعنصر الرضا موافقة صاحب البيانات على عملية جمع بياناته أو معالجتها أو حفظها أو نشرها أو إتلافها، وتنص المسودة على ضرورة الحصول على إذن مكتوب وواضح من صاحب البيانات من أجل التصرف في بياناته، مثل الإسم والجنس والجنسية والدين والسجل الطبي والمؤشرات الحيوية، والتوجهات الجنسية.

وتم التنصيص كذلك على شروط الاحتفاظ بالبيانات والإبقاء عليها بحيث تلزم الجهات المعنية بحفظ البيانات الشخصية وتخزينها في النظام الالكتروني حتى اكتمال مدة الغرض المحدَّد الذي جُمعت لأجله، وتُحدد مدة الإبقاء على البيانات بموجب القانون، وفي حالة غياب نص قانوني ينظم فترة الإبقاء على البيانات فإن المشتغلين على هذه البيانات ملزمون بإتلافها في حالة تجاوز الاحتفاظ بها مدة خمس سنوات.

وفيما يخص قيود الاستخدام فإن الجهات المعنية تتعهد بالالتزام بالغرض المحدد الذي لأجله تم تجميع هذه البيانات، إلا في حالة ماكانت هذه البيانات متاحة للعموم، وأي تشارك لهذه البيانات مع طرف ثالث لا يتم إلا بموافقة الشخص المعني، وقد نصت المسودة على السماح باستعمال البيانات بحسب الغرض المخصوص الذي حدده صاحبها، ويجرم مشروع القانون الجديد أي متاجرة بهذه البيانات مع أي طرف كان.

ثم نجد تنصيصا على وجوب الحرص على جودة البيانات بحيث تتعهد الجهات المعنية بالحفاظ على دقة المعلومات وصحتها وصدقيتها خلال عملية معالجة البيانات وتحليلها، وهناك أيضا تجريم انتهاك سرية البيانات، إذ ينبغي أن تبقى بيانات الشخص في سرية تامة، ويجوز للشخص أن يعلن عمومية بياناته ونزع صفة السرية عنها مالم ينص القانون على خلاف ذلك، وفي حالة أي اختراق لسرية البيانات فعلى الجهة المعنية



مراسلة الشخص المعني كتابيا وإعلامه بأسباب تسرب بياناته في أجل مدته 14 يوما من تاريخ وقوع الاختراق.

أما فيما يخص التوظيف المتبادل للبيانات فيتحتم على المسؤولين أن يسهروا على جعل الأنظمة الإلكترونية المخزِّنة للبيانات قابلة للاستعمال المتبادَل وعلى ضرورة موائمتها مع البرمجيات القانونية.

ونجد مسودة القانون الجديد قد تطرقت لمسألة أمن البيانات بحيث على الجهات المعنية أن توحّد قوانينها الداخلية المتعلقة بحماية البيانات الشخصية كإجراء أمني ووقائي، وعلى المشتغلين على البيانات كذلك أن يحرصوا على أمن البيانات الشخصية مادامت في حوزتهم ومنع أي سوء استعمال لها، وذلك عبر تشفير البيانات المخزنة، رغم أن القانون لم يتطرق إلى طريقة تشفير هذه البيانات، بالإضافة إلى الحرص على مداومة عملية المحاسبة والتدقيق في جميع التصرفات الصادرة.

ويحق للشخص بموجب قانون حماية البيانات الجديد أن يدخل بياناته الشخصية ويقوم بتحديثها، ويمكنه طلب إتلاف بياناته إذا استنفذت الغرض الذي جُمعت لأجله، أو في حال انتهاء مدة التخزين المتفق عليها، كما يحق للشخص طلب إلاستغناء عن معلوماته، بحيث يحق للأشخاص طلب حذف معلومات غير دقيقة تخصهم من مزودي الأنظمة الالكترونية، وذلك بعد الحصول على أمر من المحكمة.

وقد قامت الحكومة الإندونيسية كشأن بعض دول المنظمة بابتكار تطبيق خاص يعين على حسن تطبيق تدابير التباعد الجسدي اسمه Peduli Lindungi[39] (رعاية وحماية) يمكّن هذا التطبيق من مراقبة المصابين وتتبع الحالات المشكوك في إصابتها من خلال آلية متابعة على الانترنيت تتحكم فيها وزارة الصحة، ويقوم التطبيق الهاتفي بحفظ بيانات الأماكن التي زارها صاحب الهاتف والأشخاص الذين

39. https://pedulilindungi.id/.



خالطهم، بحيث يسهل رصد المخالطين والتواصل معهم من أجل أن يلتزموا بالحجر الصحي لتبيُّن إمكانية إصابتهم، وقد صرح وزير الصحة الاتصال وتكنولوجيا المعلومات بأن البيانات المُجَمَّعة من خلال التطبيق محمية تماما[40].

2. سياسة حماية البيانات الشخصية في المملكة العربية السعودية

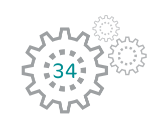
حرصت المملكة العربية السعودية على الانخراط الفعال في الحركية الرقمية العلمية التي تطبع هذا العصر وذلك عبر العمل على الاستفادة من الفرص الواعدة التي توفرها هذه التكنلوجيا الجديدة في الابتكار وتنمية الاقتصاد بحيث اعتبرت بمثابة ثروة جديدة، مما عزز موقع المملكة على الساحة الرقمية بتنظيمها للقمة العالمية للذكاء الاصطناعي[41] التي تشكل ملتقى سنوي عالمي لتبادل الخبرات وعقد الشراكات بين الجهات والشركات الفاعلة في عالم البيانات والذكاء الاصطناعي على الصعيدين المحلي والدولي، والتي كان من المزمع تنظيمها في المملكة العربية السعودية في نهاية شهر مارس 2020م بالرياض، وتم تأجيلها إلى 14-15 شتنمبر من هذا العام.

وقامت المملكة بإحداث الهيئة السعودية للبيانات والذكاء الاصطناعي[42] المعروفة أختصاراً باسم سدايا (SDAIA) وهي هيئة حكومية سعودية أنشئت بأمر ملكي في 30 أغسطس 2019، وترتبط مباشرةً برئيس مجلس الوزراء، فيما يرأس مجلس إدارتها نائب رئيس مجلس الوزراء، وستعمل الهيئة على تطوير أنظمتها الأساسية للبيانات، من خلال حماية حرية البيانات وخصوصيتها وتصنيفها وتبادلها، وتنقسم الهيئة إلى ثلاث أذرع :

40. https://jakartaglobe.id/news/minister-encourages-indonesians-to-install-covid19-surveillance-app/.

41. https://www.theglobalaisummit.com/index-ar.html.

42. https://sdaia.gov.sa/.



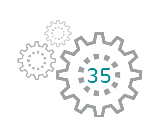
- مركز المعلومات الوطني : يضم البيانات الحكومية لدعم اتخاذ القرارات، وهو بمثابة ذراع تشريعي يختص بحوكمة البيانات الحكومية في الوزارات والجهات الحكومية من حيث الجودة، ويعمل على حماية البيانات لضمان الخصوصية والتنافسية استنادا إلى الأطر واللوائح التنظيمية التى يتم وضعها من قبل مكتب البيانات في الهيئة.

- مكتب إدارة البيانات الوطنية الجهة التنظيمية الوطنية : مهمته تعزيز السياسات المرتبطة بالعدالة والشفافية، وهو مثابة ذراع تنفيذي تسند إليه مهمة جمع وتخزين وتسهيل الوصول للبيانات الحكومية. وتحليل البيانات المتوفرة من الجهات الحكومية المختلفة بناء على طلبات الجهات المستفيدة. هذه الأعمال تخضع لتشريعات مكتب البيانات بالهيئة بتنسيق مع إدارات البيانات بالجهات الحكومية المعنية.

- المركز الوطني للذكاء الاصطناعي : الذي سيعمل على تعزيز تنفيذ إستراتيجية الذكاء الاصطناعي والتوصل إلى أحدث الخبرات والحلول في هذا المجال، وهو بمثابة ذراع إبتكاري للهيئة، يهتم ببناء القدرات في مجال الذكاء الاصطناعي عبر التدريب والبرامج التوعوية، وتقديم البحوث والإستشارات، وتطوير انظمة وتطبيقات تستخدم تقنيات الذكاء الاصطناعي للجهات الحكومية.

زيادة على ذلك فقد أصدر المركز الوطني الاسترشادي لأمن المعلومات بهيئة الاتصالات وتقنية المعلومات سبعة إصدارات توعوية جديدة متعلقة بأمن المعلومات تستهدف مستخدمي خدمات الاتصالات وتقنية المعلومات، تناولت فيها موضوع أمن المعلومات تناولاً شاملاً، واستعرضت من خلاله عدداً من القضايا المهمة بهذا الخصوص كمعالجة موضوعات أمن الشبكات اللا سلكية، وسبل حماية البريد الإلكتروني، وسبل حماية الخصوصية في العالم الرقمي، بالإضافة إلى تناولها موضوع الرسائل الاقتحامية (SPAM) من خلال استعراض أشهر أنواعها وطرق الحماية منها.

43. https://www.citc.gov.sa/ar/mediacenter/awarenesscampaigns/Pages/PR_AWR_003.aspx.

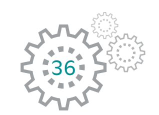


وتتطرق هذه الإصدارات كذلك إلى حماية الأطفال من أخطار شبكة الإنترنت، مستعرضة في هذا السياق عدداً من النصائح لحماية الجهاز الشخصي من مخاطر الإنترنت، بالإضافة إلى تناولها ظاهرة التصيد الإلكتروني من خلال تعريفه، وتبيان أضراره المحتملة مع تبيان أوجه الوقاية منه، ويأتي نشر هذه الإصدارات بوصفه أحد مهمات الهيئة التوعوية تجاه المستخدمين في المملكة العربية السعودية بكل ما يحيط بقطاع الاتصالات وتقنية المعلومات من مفاهيم، وسلوكيات، وممارسات يجدر التعريف بها، ومعالجتها بما يعزز من مفهوم الممارسات الآمنة لتقنيات الاتصالات وتقنية المعلومات.

وقامت الهيئة السعودية للبيانات والذكاء الاصطناعي «سدايا» بإطلاق تطبيق «تباعد»[44] لمساندة الجهود الحكومية في مواجهة فيروس كورونا واعتمدته وزارة الصحة، بموجب النظام الصحي ولوائحه التنفيذية في المملكة العربية السعودية، وذلك لتحقيق الغاية الصحية والسلامة المتوخاة من تطوير التطبيق عبر إشراك الأفراد في السيطرة على تفشي جائحة فيروس كورونا المستجد، والحد من التوسع في انتشاره، وسعيًا إلى الخفض التدريجي للقيود المفروضة على الحياة الاجتماعية والأنشطة الأخرى، ويعتبر تطبيق (تباعد) وسيلةً لإشعار المخالطين للمصابين بفيروس كورونا المستجد، حيث يمكن للأفراد تحميل التطبيق واستخدامه لتحقيق الغاية الصحية التي طُوّر لأجلها.

ويقوم التطبيق بإرسال بيانات معرفة مموهة إلى الجوالات الذكية المستخدمة للتطبيق، التي سُجلت خلال فترة الاختلاط بمصاب فيروس كورونا المستجد، مصحوبةً ببيانات أجهزة الأشخاص المصابين، وذلك حسب سياسات شركتي (غوغل وأبل) العالميتين، مع الحفاظ على كامل خصوصية المستخدمين، ويمكن التطبيق المستخدِم من الحصول على الإشعارات المباشرة والاستباقية حال اكتشاف أي إصابة مسجلة، لغرض طلب الدعم الصحي المباشر من وزارة الصحة.

44. https://tabaud.sdaia.gov.sa/.



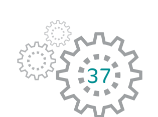
3. حماية البيانات الخاصة في دولة الإمارات العربية المتحدة

تطبق دولة الإمارات القانون الاتحادي رقم (12) لسنة 2016 المتعلق بمكافحة جرائم تقنية المعلومات وغيره من القوانين المتعلقة بحماية الخصوصية ومنع انتهاك البيانات الشخصية عند استخدام وسائل التواصل الاجتماعي، حيث تحظر المادة 21 من هذا القانون كل استخدام شبكة معلوماتية أو أي نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات في الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانوناً بإحدى الطرق التالية:

استراق السمع، أو اعتراض، أو تسجيل أو نقل أو بث أو إفشاء محادثات أو اتصالات أو مواد صوتية أو مرئية والتقاط صور الغير أو إعداد صور الكترونية أو نقلها أو كشفها أو نسخها أو الاحتفاظ بها، نشر أخبار أو صور الكترونية أو صور فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية.

وتحظر المادة 22 من القانون كل من استخدم، بدون تصريح، أي شبكة معلوماتية، أو موقعاً الكترونياً، أو وسيلة تقنية معلومات لكشف معلومات سرية حصل عليها بمناسبة عمله أو بسببه.

كما صاغت دولة الإمارات سياسية خاصة سمتها «سياسة إدارة النفاذ للإنترنت (IAM)» وهي سياسة تطبقها هيئة تنظيم الاتصالات بالتنسيق مع المجلس الوطني للإعلام ومزودي خدمات الإنترنت المرخص لهم في الدولة، ووفقاً لهذه السياسة يتم حجب الوصول إلى المواقع والصفحات التي تحتوي على محتوى محظور ويشمل ذلك النصب والاحتيال، والتصيد الإلكتروني، وانتهاك الخصوصية، وانتهاك حقوق الملكية الفكرية، حيث يتم حجب الوصول إلى المواقع والصفحات التي تحتوي على محتوى محظور من قبل مزودي خدمات الإنترنت في دولة الإمارات العربية المتحدة بعد رصدها والإبلاغ عنها من قبل المتعاملين.

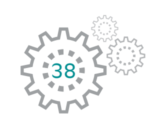


وينص قانون العقوبات الإماراتي في المادة 378 على عقاب كل من اعتدى على حرمة الحياة الخاصة أو العائلية للأفراد وذلك إذا ارتكب أحد الأفعال التالية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه :

- استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه محادثات جرت في مكان خاص أو عن طريق الهاتف أو أي جهاز آخر.
- التقط أو نقل بجهاز أيا كان نوعه صورة شخص في مكان خاص، فإذا صدرت الأفعال المشار إليها في الحالتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع فإن رضاء هؤلاء يكون مفترضا.

وقامت دولة الإمارات باعتماد حلول ذكية لمكافحة كوفيد 19 للكشف عن الحالات وتتبعها، والسيطرة على انتشار الوباء، ومن أبرز هذه الحلول الذكية تطبيق «الحصن» الذي يتيح معرفة الأشخاص المخالطين للحالات المصابة بالفيروس كما يوفر خاصية الإطلاع على نتائج الفحوصات الطبية بسهولة[45]، ويعتبر تطبيق الحصن الإماراتي المنصة الرقمية الرسمية الخاصة باختبارات فيروس كورونا المستجد (كوفيد 19) في دولة الإمارات، ويعمل على معرفة ما إن كان الشخص على مقربة من أشخاص قاموا بمخالطة أو التعامل مع أشخاص ثبتت إصابتهم بفيروس كوفيد 19، كما يتيح التطبيق للأشخاص الذين يخضعون لاختبارات الكشف عن الفيروس بتلقي نتائج اختباراتهم مباشرة على هواتفهم، ويعتمد التطبيق على استخدام الإشارات قصيرة المدى الخاصة بتقنية البلوتوث وذلك في حال توفر التطبيق ذاته على الهواتف المحمولة للأشخاص الأخرى، حيث تتبادل الهواتف البيانات الوصفية التي يتم تخزينها بعد ذلك على تطبيق الحصن بصيغة مشفرة موجودة فقط على هواتف المستخدم، ويمكن للجهات الصحية المختصة من خلال هذه البيانات

45. https://www.ncema.gov.ae/alhosn/index-ar.html.



التعرف بسرعة على الأشخاص المعرضين لخطر انتقال العدوى إليهم ليتم التواصل معهم واختبارهم.

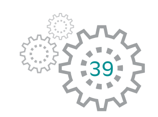
ومن الحلول الذكية كذلك إنشاء منصة «الدكتور الافتراضي لكوفيد 19»، والتي من خلالها يمكن للأشخاص تقييم الأعراض المرضية التي تظهر عليهم وما إذا كانت تلك الأعراض مرتبطة بفيروس كورونا المستجد «كوفيد 19»، أم لا، كما تقوم هذه المنصة بطرح المنصة على المريض مجموعة من الأسئلة وبناء على إجابات الشخص يستنتج الدكتور الافتراضي فيما إذا كان المريض يُعاني من احتمالية إصابته بمرض كوفيد 19.

4. مقتضيات حماية الخصوصية في القانون المغربي وآليات حماية المعطيات الشخصية

انضم المغرب منذ استقلاله إلى المجتمع الدولي في الدفاع عن الحقوق والحريات عبر مصادقته على الاتفاقيات الدولية لحماية حقوق الإنسان بصفة عامة، وحماية الحق في الخصوصية بصفة خاصة، كما عمل على تطوير ترسانته التشريعية الداخلية من أجل تكريس حماية هذه الحقوق، حيث نص من خلال المادة 24 من الدستور على ما يلي : «لكل شخص الحق في حماية حياته الخاصة، لا تنتهك حرمة المنزل، ولا يمكن القيام بأي تفتيش إلا وفق الشروط والإجراءات التي ينص عليها القانون، لا تنتهك سرية الاتصالات الشخصية كيفما كان شكلها، ولا يمكن الترخيص بالاطلاع على مضمونها أو نشرها، كلا أو بعضا، أو باستعمالها ضد أي كان، إلا بأمر قضائي، ووفق الشروط والكيفيات التي ينص عليها القانون».

ولم يقتصر الأمر على الوثيقة الدستورية، بل تعززت هذه الحماية من خلال إصدار قانون خاص يتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي[46]، حيث نظم من خلاله آليات التشفير

46. ظهير شريف رقم 15.09.1 صادر بتاريخ 18 فبراير 2009 المنشور بالجريدة الرسمية عدد5711 بتاريخ 23 فبراير 2009.



والتوقيع الإلكتروني وتحديد القيمة القانونية للوثائق والالتزامات الالكترونية، ومنع معالجة المعطيات الشخصية لأي فرد دون الحصول على موافقته ورضاه، ومنحه الحق في إخباره بخصائص المعالجة المنجزة[47]، كما له الحق في الولوج والاستفسار عن المعطيات المعالجة والجهات التي أرسلت إليها[48]، وممارسة حق التصحيح وتحيين المعطيات المتعلقة به أو إزالتها أو منع الولوج إليها إذا كانت ناقصة أو غير صحيحة[49]، كما فرض هذا القانون على المسؤول عن معالجة البيانات الشخصية احترام مبدأ التناسب دون الإفراط في المعطيات، وألزمه بضرورة التحقق من جودة المعطيات وصحتها، واحترام مدة حفظ المعطيات لتحقيق الغاية من المعالجة التي جُمِعت من أجلها، وكذا التزامه بالسر المهني[50]، وقد أفرد القانون رقم 08.09 لعدم احترام الإجراءات السابقة عقوبات إدارية[51] وجنائية[52] حسب نوع المخالفة.

ولضمان حسن تطبيق هذا القانون أحدث المشرع لجنة وطنية لمراقبة حماية المعطيات ذات الطابع الشخصي[53]، مهمتها التحقق من أن عملية معالجة المعطيات الشخصية تتم وفق القانون ولا تمس بالحياة الخاصة لأصحابها.

وبالرغم من فرض المغرب لحالة الطوارئ الصحية بتاريخ 20 مارس 2020، إثر تسجيل حالات إصابات بفيروس كورونا على مواطنيه، ورغم أن قانون 08.09 المتعلق بحماية المعطيات الشخصية قد استثنى تطبيق مقتضيات هذا القانون بخصوص المعطيات المحصل عليها والمعالجة لمصلحة الدفاع الوطني والأمن الداخلي والخارجي للدولة[54]،

47. المادة 6 من قانون 08.09 المتعلق بحماية المعطيات ذات الطابع الشخصي.

48. المادة 7 من قانون 08.09 المتعلق بحماية المعطيات ذات الطابع الشخصي.

44. https://tabaud.sdaia.gov.sa/

49. المادة 8 من قانون 08.09 المتعلق بحماية المعطيات ذات الطابع الشخصي.

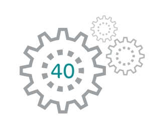
50. المادة 23 من قانون 08.09 المتعلق بحماية المعطيات ذات الطابع الشخصي.

51. المادة 64 من قانون 08.09 المتعلق بحماية المعطيات ذات الطابع الشخصي.

52. المادة 55 وما يليها من قانون 08.09 المتعلق بحماية المعطيات ذات الطابع الشخصي.

53. الباب الرابع من قانون 08.09 المتعلق بحماية المعطيات ذات الطابع الشخصي حدد أعضاء واختصاصات اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي وقد تم تنصيبها بتاريخ 31 غشت 2010.

54 المادة 12 من قانون 08.09 المتعلق بحماية المعطيات ذات الطابع الشخصي.



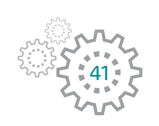
فإن المغرب يؤكد على احترام الخصوصية أثناء معالجة المعطيات الشخصية، وقد أكدت ذلك اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي بعد اعتماد المديرية العامة للأمن الوطني لتطبيق الكتروني يمكّن من مراقبة وتتبع المواطنين داخل نقاط المراقبة الأمنية، لمعرفة مدى احترام قانون الطوارئ الصحي ورصد المخالفين، حيث دعت اللجنة إلى الشفافية والسهر على التخلص من المعطيات المُجمّعة عند الخروج من حالة الطوارئ[55]، كما تكرّس هذا التوجّه في تطوير تطبيق «وقايتنا»[56]، وهو تطبيق مغربي متوفر بالمجان للإشعار باحتمال التعرض لفيروس كورونا المستجد «كوفيد 19» يساعد على إشعار المستعمل في حالة تواجد مستعمل آخر بالقرب منه خلال 21 يوما الأخيرة تأكدت إصابته بالفيروس، هذا التطبيق الذي يقوم بحفظ المعطيات المتعلقة بالمستعملين في نطاق جغرافي محدد وفي مدة زمنية معينة بطريقة مشفرة، دون أي معالجة للبيانات المتعلقة بالموقع الجغرافي للمستعمل التي تشكل انتهاكا للحياة الشخصية لصاحب التطبيق، وتقع مهمة رصد الحالات المصابة على عاتق فريق متخصص من وزارة الصحة المغربية عُهد إليه القيام بالاختبارات اللازمة لأجل تفادي الإشعارات المزيفة وتأكيد إصابة الشخص المعني، وذلك لتفادي الإشعارات المزيفة حتى لا يصبح التطبيق عديم الفائدة، ويندرج هذا التطبيق ضمن الاستراتيجية الوطنية للتصدي لجائحة لفيروس كورونا المستجد، وتم تطويره من طرف فرق متعددة التخصصات تنتمي لوزارة الصحة ووزارة الداخلية، وبتعاون مع الوكالة الوطنية لتقنين الاتصالات ووكالة التنمية الرقمية[57]، وكذا بمساهمة تطوعية لمقاولات وشركات مغربية خبيرة في مجالاتها، في احترام تام للمبادئ التالية :

- استخدام التطبيق حصرا على أساس طوعي.
- دعم النظام الصحي، خاصة لترشيد الموارد بهدف تعزيز سياسة الكشف المبكر وإخبار المواطنين.

55 مقال منشور، بموقع فرنسا24، تحت عنوان فيروس كورونا: تطبيق رقمي لضبط المخالفين أثناء حالة الطوارئ الصحية بالمغرب،www.france24.com

56 https://www.wiqaytna.ma/

57. https://www.anrt.ma/.

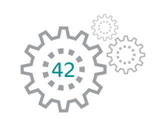


- مراقبة السلطات الصحية لإعدادات خوارزميات حساب التنبيه.
- استخدام آلية التتبع «tracing» بدون آلية التعقب «tracking».
- إخبار المَستخدِم.
- حصر الولوج إلى المعطيات في الأشخاص المؤهلين.
- الالتزام بعدم استخدام المعطيات لغايات أخرى غير تلك المصرح بها.
- الالتزام بإتلاف المعطيات التي تم تجميعها وانتاجها فور الخروج من حالة الطوارئ الصحية، باستثناء المعطيات التي يمكن أن تساهم، دون أن تسمح بالتعرف على الأشخاص الذاتيين، في البحث العلمي.
- التصريح بعدم استخدام صندوق أسود (black box).
- الالتزام بجعل الشفرة المطورة متاحة لأغراض المراقبة والتدقيق.

وقد فَرَضَ تدبير جائحة فيروس COVID-19 اتخاذ عدة إجراءات تنظيمية وتداولية، فيما يخص حماية المعطيات ذات الطابع الشخصي من قَبيلِ :

- تقليص مدة بث اللجنة الوطنية بخصوص التصريحات وطلبات الإذن التي تتوصل بها، خاصة تلك التي تتعلق بتدبير الوباء والتي يتم معالجتها عن طريق الاستعجال.
- تأطير العمل عن بعد في قطاع العلاقة مع الزبناء،
- قياس درجة الحرارة بهدف الولوج إلى مكان العمل أو الأماكن العامة،
- أحكام استثنائية لتدبير الحسابات المصرفية عن بعد.
- مختلف التطبيقات الإلكترونية لرصد عدم الامتثال للحجر الصحي،

وقد تلقت اللجنة الوطنية، بتاريخ 27 أبريل 2020، طلبا بخصوص البت في امتثال التطبيق الذي يحمل اسم «وقايتنا» (WIQAYATNA) لمقتضيات القانون 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، بما في ذلك الغاية المتوخاة



والمتمثلة في دعم التدبير الصحي لانتشار جائحة Covid-19، حيث تقوم هذه اللجنة منذ بداية الأزمة الصحية، باعتماد أنظمة يقظة متعددة تكفل لها نجاعة اتخاذ قراراتها، وذلك من خلال :

- تتبع الأبحاث والتنبيهات والتوصيات الدولية (بما في ذلك توصيات لجنة الاتفاقية رقم 108 التابعة لمجلس أوروبا وتوصيات الشركاء الدوليين الذين ساعدوا اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي على الحصول على بعض المعلومات التكنولوجية)،
- تتبع ملاحظات ومخاوف وتوصيات المواطنين على المستوى الوطني،
- الاستماع إلى الخبراء التقنيين الوطنيين والدوليين حول هذا الموضوع،
- قيام اللجنة الوطنية بالأبحاث الخاصة بها.

وقد ظلت اللجنة الوطنية رهن إشارة السلطات والمواطنين من أجل تعزيز الثقة الرقمية الضرورية لتشجيع رقمنة المجتمع، ودعم تدبير المخاطر الصحية والحفاظ على الحياة الاقتصادية في احترام للحياة الخاصة.

بناء على ذلك، قررت اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي، كما نصت عليه المادة 42 من القانون 09.08، تشكيل لجنتين خاصتين :

- اللجنة الخاصة بـ «استراتيجية الثقة الرقمية والأخلاقيات الرقمية» تتكون من خبراء وشخصيات متخصصة في المجال الرقمي، كما تم الاعلان عنه في نهاية سنة 2019، ستعطى الأولوية سنة 2020 لحماية المعطيات المتعلقة بالصحة، وتندرج ضمن اختصاصات هذه اللجنة، المواضيع المتعلقة بأخلاقيات العلوم البيولوجية في المجال الرقمي.
- اللجنة الخاصة بـ «الثقة الرقمية التنفيذية»، تتكون من خبراء مغاربة يقدمون الاستشارة والدعم للجنة الوطنية في مهمات المراقبة والتحقق المخولة لها بموجب المادة 30 من القانون 09.08 [58].

58. https://www.cndp.ma/ar/presse-et-media/communique-de-presse/674-communique-de-presse-du-12-05-2020.html.

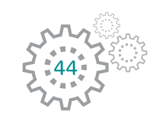


وقد ساهمت هذه الأزمة الصحية في المغرب من فتح أفق أوسع للتفكير في مسائل حماية الخصوصية في ظل الاستعمال المتعاظم للوسائل التقنية المتقدمة المعينة على احتواء الوباء، وأكدت اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي على تبني موقف واضح ونوعي خلال فترة الأزمة الصحية من أجل التوفيق بين ضرورة حماية الحياة الشخصية ودفع مخاطر الوباء، حتى تدبَّر هذه المرحلة الاستثنائية بإجراءات واضحة وبمقاربة تشاركية ومنهجية وفق الضوابط القانونية، وتظل ساحة النقاش والتفكير مفتوحة في وجه كل الفاعلين المهتمين بقضايا الخصوصية وحقوق الإنسان من أجل تعميق النقاش وإثرائه، ما يستوجب تظافر جهود كل الشركاء المنخرطين في تدبير هذه الأزمة من أطر صحية ومبتكرين ومهندسين ومجتمع مدني، من أجل التوصل إلى أطر قانونية تستجيب للمعايير الدولية و القانونية الكفيلة بحفظ هذا الحق المهم من حقوق الإنسان من كل خطر يهدده، خصوصا وأن المغرب قد أخذ على عاتقه الانخراط في مسار توطيد ثقافة حقوق الإنسان من خلال مؤسسة المجلس الوطني لحقوق الإنسان[59]، وهو مؤسسة دستورية مستقلة رائدة في منطقة الشرق الأوسط وشمال أفريقيا تأسست سنة 1990 ومنحها الدستور الجديد للمملكة صلاحيات أوسع لجعلها أكثر استقلالية من أجل حماية حقوق الإنسان وكذلك لتعزيز المبادئ والقيم الديمقراطية في المجتمع.

وقد انخرط المغرب في سياسة التحول الرقمي بما يحترم حماية المعطيات الشخصية ويحمي المواطن، وذلك عبر إطلاق برنامج «داتا ثقة» «TIKA-DATA» في ثلاث صيغ :

- «داتا ثقة» الخاصة بالشركات
- «داتا ثقة» الخاصة بالقطاع العام
- «داتا ثقة» الخاصة بالجمعيات والمنظمات غير الحكومية

59. https://www.cndh.ma/.



وسيمكن برنامج «داتا ثقة» في صيغه الثلاث من تغيير النماذج الفكرية المعمول بها بدلا من الاكتفاء بفهم الإجراءات التي يتعين اتخاذها من أجل الامتثال لمقتضيات القانون 08.09، مما سيمكن المستخدم من المساهمة بشكل استباقي في تغذية المقاربات الميدانية للجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي من أجل الإجابة عن الإشكاليات المستجدة المرتبطة بـ «اقتصاد المعطيات» وتشجيع الابتكار وتحفيز الاستثمار[60].

5. تطبيق «إحمي» وحماية الخصوصية من خلال القانون التونسي

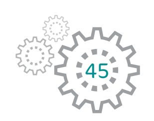
تُعد الجمهورية التونسية من الدول السباقة في اعتماد قانون خاص بحماية المعطيات الشخصية، حيث أصدرت القانون عدد 63 سنة 2004 المتعلق بحماية المعطيات الشخصية الذي تضمن الإجراءات والتدابير التي يجب احترامها أثناء معالجة البيانات الشخصية، كما حدد بموجب الفصل 21 من قانون عدد 63 واجبات المسؤول عن المعالجة، كما أعطى للأشخاص بموجب الفصل 32 حق النفاذ، حيث يحق للمعني بالأمر أو ورثته الاطلاع على جميع المعطيات الشخصية الخاصة به وطلب إصلاحها أو إتمامها أو تعديلها، كما تم إحداث الهيئة الوطنية لحماية المعطيات الشخصية[61]، كما رتب عقوبات[62] على مرتكبي الجرائم الماسة بحماية المعطيات الشخصية والتي حددها المشرع ضمن القانون عدد 63 لسنة 2004.

وأكدت الهيئة الوطنية لحماية البيانات الشخصية أن التحديات التي تواجهها تونس خلال جائحة كورونا غير مسبوقة، وأن التصدي لهذا الفيروس يقتضي تجميع المعلومات وتبادلها بسرعة وتحيين طرق عملها على ضوء المستجدات، وعليه فمن حيث المبدأ لا تمانع الهيئة

60. http://www.maroc.ma/fr/actualites/la-cndp-met-en-place-les-programmes-data-tika-pour-la-protection-des-donnees-caractere.

61. الفصل 75 من القانون عدد 63 المتعلق بحماية المعطيات الشخصية.

62. الباب السابع من القانون عدد 63 المتعلق بحماية المعطيات الشخصية.



من تبادل المعطيات الشخصية المتعلقة بالصحة مع ضرورة احترام الفصل 49 من دستور سنة 2014 [63]، الذي يقر بوجوب احترام الموازنة بين ممارسة الدولة لصلاحيات السلطة العمومية مقابل العمل على احترام حقوق الأفراد ، كما شددت على تجنب معالجة كم من المعطيات أكثر مما هو ضروري أثناء التدريس عن بعد[64].

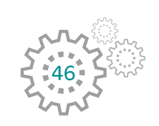
وقد قامت دولة تونس بإطلاق تطبيق «إحمي»[65] للحدّ من انتشار فيروس كوفيد 19 في البلاد والذي يمكن من تنبيه الأشخاص الذين اقتربوا من حالات مصابة عبر تقنية «بلوتوث»، ويختلف هذا التطبيق عما قدمته كل من شركة آبل وغوغل كحلّ لعمليات تعقب مسارات حاملي المرض، بحيث ينبه «المرصد الوطني للأمراض الجديدة والمستجدة» ـ وهو مؤسسة حكومية ـ بتنبيه الأشخاص الآخرين الذي اقتربوا منه في طريقهم او التقوه انطلاقا من جملة المعلومات التي يخزنها الهاتف ويرسلها إلى الجهاز المركزي.

استنادا على الأمثلة المذكورة فإن على الدول أن تبقى ضامنة لحق الخصوصية بالرغم من فرض حالة الطوارئ الصحية، وذلك بتطبيق العقوبات التي ترتبها قوانينها على مرتكبي الجرائم أثناء معالجة واستخدام المعطيات الشخصية وإن كان ذلك من أجل التصدي للفيروس، وقد أكد جو كاناتاسي، أحد خبراء الأمم المتحدة والمقرر الخاص المكلف بالحق في الحياة الخاصة في بيان جنيف الصادر بتاريخ 16 مارس 2020 : «بأن إعلان حالة الطوارئ بسبب وباء كوفيد 19... لا ينبغي أن يستخدم لاتخاذ تدابير قمعية تحت ذريعة حماية صحة السكان واستغلاله للتصدي للمدافعين عن حقوق الإنسان... ويجب أن تكون الغاية من القيود المفروضة لمكافحة الفيروس هي خدمة الصالح

63. ينص الفصل 49 من دستور 2004 التونسي على ما يلي : «يحدد القانون الضوابط المتعلقة بالحقوق والحريات المضمونة بهذا الدستور وممارستها بما لا ينال من جوهرها, ولا توضع هذه الضوابط إلا لضرورة تقتضيها دولة مدنية ديمقراطية وبهدف حماية حقوق الغير، أو لمقتضيات الأمن العام، أو الدفاع الوطني، أو الصحة العامة، أو الآداب العامة، وذلك مع احترام التناسب بين هذه الضوابط وموجباتها. وتتكفل الهيئات القضائية بحماية الحقوق والحريات من أي انتهاك. لا يجوز لأي تعديل أن ينال من مكتسبات حقوق الإنسان وحرياته المضمونة في هذا الدستور».

64. مقال منشور بموقع www.tn24.tn تحت عنوان كورونا : توصيات هيئة حماية المعطيات الشخصية.

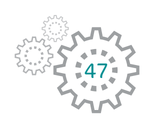
65. https://www.africanchallenges.com/tybusue-l-application-ihmi-proteger-pour-reduire-la-propagation-du-virus-corona/.



العام في إطار المشروعية... ولمنع مثل هذه السلطات من الإفراط في اعتماد سياسات أو منظومات قانونية في هذا الخصوص بدعوى الاستجابة لضرورة الاستعجال»[66]، كما أكدت منظمة اليونسكو على أن التقنيات الرقمية مثل الهواتف المحمولة ووسائل التواصل الاجتماعي والذكاء الاصطناعي، يمكن أن تلعب دوراً مهما في المعركة ضد الأوبئة، من خلال مراقبة انتشار الفايروس وتأثير ذلك على سلوك الأشخاص، وأن من الضروري التأكد بأن المسائل الأخلاقية والاجتماعية والسياسية المتعلقة باستخدام هذه التقنيات يتم معالجتها بطرق خاضعة للقانون، كما يجب دائما احترام حقوق الإنسان وتحقيق الموازنة بين قيم الحياة الخاصة والاستقلالية مع قيم السلامة والأمن[67].

66. مقال منشور بموقع www.news.tn.

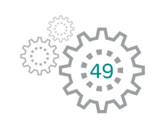
67. بيان صادر عن منظمة اليونسكو تحت عنوان كوفيد 19 : الاعتبارات الأخلاقية من منظور عالمي بتاريخ 26 مارس 2020، منشور بالموقع الإلكتروني : www.ar.unesco.org



المحور الثالث : تحديات التأطير القانوني لحماية البيانات الشخصية في استخدامات الذكاء الاصطناعي ـ التجارب والاجتهادات ـ

نشهد اليوم تعاظم النقاش حول مسألة تدعيم أخلاقيات الذكاء الإصطناعي بالنظر إلى الوضعية الحالية الحرجة، غير أن هذه الأخلاقيات تصطدم بحالات الطوارئ حين يكون تدبير الأزمات أولى من التفكير في الحلول السليمة، نظرا لاختلاف منظورات التعاطي مع الأزمات بين التدبير اللحظي وبين التوصل إلى الحلول المستديمة، وهذا ما شهدناه حاليا حين تم توسيع نطاق استعملات الذكاء الإصطناعي بشكل غير مسبوق، حيث أدى هذا الاعتماد المتعاظم إلى الكشف عن عجز الاقتصار على الأطر القانونية منفردة ومحدوديتها في مسايرة مجمل هذه الاستعمالات والإحاطة بها، وقد اقتصر جهد المشتغلين على الجوانب الأخلاقية والقانونية لتقنيات الذكاء الإصطناعي على وضع أطر أخلاقية ومبادئ عامة، لكن هذه المبادئ القانونية لا تدلنا على ما ينبغي فعله حين الوقوع في حالة تنازع المبادئ واصطدامها، مثال ذلك التقاء مبدأ حفظ حياة الأشخاص بمبدأ آخر مهم هو مبدأ النزاهة واحترام الخصوصية حين يتعلق الأمر بالمعلومات الشخصية للأفراد، ولأجل تخفيف حدة هذا التنازع فلابد من إدارة حوار بناء مع مختلف الفاعلين في ميدان الذكاء الإصطناعي والخوارزميات بصفة عامة، وهو أمر يتطلب استعدادا وجهدا، غير أن الأزمات تَعتبِر الوقت عنصرا ضاغطا ومؤثرا ليس لصالحها، وهنا نجد أنفسنا بين ثنائية الانفعال اللحظي التي تقتضي إيجاد حلول آنية ولحظية، وبين واجب التفاعل المُتعقل الذي يراعي ظروف الواقع ويستحضر الإمكانات والمعيقات، لكن هل هذا الوضع يعني التخلي نهائيا عن هذه الأخلاقيات حين الأزمات ؟

على العكس من ذلك تماما فإن الأزمة الحالية تؤكد على ضرورة مضاعفة جهود المشتغلين على الجانب الأخلاقي والحقوقي للذكاء الاصطناعي، عبر ضرورة إيجاد حلول وقواعد مؤطرة تصاغ بنفس



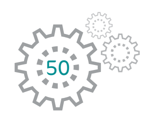
السرعة التي يتم فيها ابتكار حلول تكنولوجية تعتمد الخوارزميات في تصميمها، وهو ما يستدعي استنهاض جهود القانونيين والمهتمين بأخلاقيات الذكاء الإصطناعي والسعي قدما نحو مسايرة النمو السريع في استعمالات الذكاء الإصطناعي حتى لا يبقى التأطير القانوني متخلفا عن ركب التطور التكنولوجي وتابعا له فقط، بل ينبغي أن يتجاوز الانفعال إلى المسايرة والاستباق.

لأجل هذا الغرض لابد لأخلاقيات الذكاء الإصطناعي أن تسترشد بثلاثة أمور أساسية :

1. ضرورة التفاعل البناء والنقدي بدل الإنفعال وإبداء القلق تجاه هذه التقنية.
2. إيجاد قواعد وقيم أخلاقية صلبة كفيلة بضمان سلامة استخدامات أنظمة الذكاء الإصطناعي.
3. العمل على بناء الثقة العامة لدى المجتمع عبر الإشراف والرقابة المؤسَّسَين والمستقلين.

ويتم التفاعل البَنّاء عبر جعل المسألة الأخلاقية ضمن مراحل إنشاء هذه الخوارزميات بحيث تصير دراسة الجوانب الأخلاقية والقانونية مرحلة مهمة ضمن مراحل الإبتكار ودراسة المشاريع، وليست فقط مرحلة بعدية لاحقة على انتهاء مرحلة الإخراج النهائي للمشاريع التكنولوجية، وهو ما من شأنه اختصار الوقت والجهد[68]، ويتحقق هذا المطلب كذلك عبر تنويع مصادر الخبرة المنجزة للمشروع والتكوين المستمر للمبتكرين والشركات على هذه الجوانب القانونية والأخلاقية، وهنا نكون أمام ضرورة تنمية حس المسؤولية في البحث والابتكار لدى المخترعين والمختبرات والشركات.

68. d'Aquin, M. et al. In Proc. 2018 AAAI/ACM Conf. AI, Ethics, and Society 54–59 (ACM, 2018).



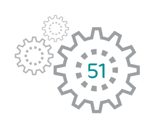
1. الفراغ القانوني المصاحب للظروف الاستثنائية والأزمات

أمام مطلب حفظ حياة الناس وتحدي انتشار الوباء، تستعين البشرية اليوم بكل الوسائل المتاحة لأجل مواجهة الأزمة الصحية الحالية بغية محاصرة الوباء وتتبع انتشاره، وفي مقدمة هذه التقنيات نجد الذكاء الاصطناعي والبيانات الضخمة وقواعد البيانات المتسلسلة، كمثال المعلومات الصادرة عن الهواتف المحمولة المتعلق بموقع الأشخاص، لذا فإن الحصول على هذه البيانات يعين على تعقب الحالات المصابة وتنبيه المواطنين من مواقع المصابين وبؤر الوباء، ما من شأنه التقليل من نسب المصابين به والتنبؤ بحركيته، وتوفّر بعض الشركات الإلكترونية خدمة اختيارية لأجل مشاركة موقع المستخدمين لأجل جمع أكبر عدد من البيانات حول تنقلاتهم وحالتهم الصحية ونشاطهم اليومي، مثل برنامج غوغل Coronavirus Mobility Reports، بالموازاة مع هذا التفاعل الرقمي مع الوباء يحذر المختصون من مغبة سوء استعمال هذه البيانات، لأن كل هذه التقنيات المبتكرة تعتمد على البصمات الرقمية للمستخدم وتلج أجهزته المحمولة، ما يشكل انتهاكا لخصوصيات المستخدمين، ويذكي المخاوف حول الإبقاء على التقنيات التي استعملت أثناء الوضع الاستثنائي الحالي إلى بعد انتهاء الجائحة[69].

من المهم للحكومات عند الحديث عن الأزمات الكبرى مثل الكوارث والأوبئة فهم منشأ الخطر ومساراته المحتملة ومدى التزام الناس بشروط الحجر الصحي، لذلك تحتاج الحكومات والمؤسسات البحثية إلى المعلومات لأجل التبصر بمآل التهديدات والتحديات من أجل صياغة الخُطط الكفيلة بالخروج من الأزمات، وتعتبر البيانات المتعلقة بمواقع تواجد المواطنين مهمة في زمن الأوبئة، لذلك اعتمدت العديد من الحكومات برامج التعقب والتتبع لمواقع تواجد المواطنين بالتعاون مع شركات الاتصالات مثل الصين وهونك كونغ وكوريا الجنوبية، وتنحو الولايات المتحدة نحو



69. https://www.healthcareitnews.com/news/covid-19-emergency-shows-limitations-nationwide-data-sharing-infrastructure.



نفس الاتجاه لأجل التفاوض مع شركة غوغل وفيسبوك قصد التنسيق في تبادل معلومات تواجد المستخدمين من أجل توظيفها في دفع مخاطر العدوى والحرص على التباعد الجسدي[70].

كما تستوجب ظروف الأزمات القيام بكل ما هو متاح لأجل دفع المخاطر المحدقة باستقرار الدول، لذلك تلجأ الحكومات إلى المراقبة والتعقب والمنع والحجر، وغيرها من الوسائل التي تستهدف حفظ حياة الناس، والتي قد يرى فيها البعض مساسا بحرية الأشخاص، لكن الظروف الاستثنائية لابد لها من إجراءات استثنائية، لذلك وقع التنصيص في العديد من الدساتير ومواثيق حقوق الانسان على المواد التي تؤطر الظروف الاستثنائية، بالإضافة إلى العهد الدولي الخاص بالحقوق المدنية والسياسية والاتفاقية الأوروبية لحقوق الانسان التي تتضمن كذلك مقتضيات تؤطر فترات الأزمات، ومن المفيد في هذا الصدد الاطلاع على الإطار المؤسسي للمجلس الأوروبي، هذه المنظمة الدولية التي تدير وتسهر على إحدى أهم المعاهدات الحقوقية الدولية للحريات الخاصة وهي الاتفاقية الأوروبية لحقوق الانسان، وقد وضع المجلس الأوروبي إجراءات واجتهادات فقهية وقضائية متقدمة متعلقة بظروف الأزمات كمثل التي نشهدها حاليا، حيث تنص المادة 15 من الاتفاقية الأوروبية لحقوق الإنسان على الاستثناءات الممكنة التي تقع على تقييد حريات المواطنين[71]، وقد تم تحيين هذه المادة مؤخرا في 31 دجنبر 2019 من طرف المجلس الأوروبي والمحكمة الأوروبية لحقوق الإنسان والتي تنص على ما يلي الاستثناءات التالية :

- حالة الحرب أو غيرها من حالات الطوارئ العامة التي تهدد حياة الأمة
- التدابير التي تقتضيها الظروف الاستثنائية

70. https://medium.com/opendatacharter/open-covid-19-data-461e1cbefbba.

71. WHO Director-General's Opening Remarks at the Media Briefing on COVID-19 - 11 March 2020 (n.d.) https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19%2D%2D-11-march-2020. Accessed 30 Mar 2020.

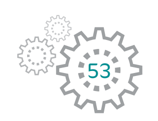


- اشتراط تناسق هذه التدابير والالتزامات الاخرى المنصوص عليها في القانون الدولي

كما تنص المادة 4 من العهد الدولي الخاص بالحقوق المدنية والسياسية على التالي :

1. «في حالات الطوارئ الاستثنائية التي تتهدد حياة الأمة، والمعلن قيامها رسميا، يجوز للدول الأطراف في هذا العهد أن تتخذ، في أضيق الحدود التي يتطلبها الوضع، تدابير لا تتقيد بالالتزامات المترتبة عليها بمقتضى هذا العهد، شريطة عدم منافاة هذه التدابير للالتزامات الأخرى المترتبة عليها بمقتضى القانون الدولي وعدم انطوائها على تمييز يكون مبرره الوحيد هو العرق أو اللون أو الجنس أو اللغة أو الدين أو الأصل الاجتماعي.
2. لا يجيز هذا النص أي مخالفة لأحكام المواد 6 و7 و(الفقرتين 1 و2) و11 و15 و16 و18.
3. على أية دولة طرف في هذا العهد استخدمت حق عدم التقيد أن تعلم الدول الأطراف الأخرى فورا، عن طريق الأمين العام للأمم المتحدة، بالأحكام التي لم تتقيد بها وبالأسباب التي دفعتها إلى ذلك. وعليها، في التاريخ الذي تنهى فيه عدم التقيد، أن تعلمها بذلك مرة أخرى وبالطريق ذاته».

ويعتبر مبدأ حفظ البيانات الشخصية مبدأ حصينا في قانون العقود، غير أن القوانين التنظيمية للحماية الشخصية كقانون الاتحاد الأوروبي لحماية البيانات تركز أساسا على الحقوق الفردية والموافقة الشخصية لصاحب البيانات، وتترك هامشا واسعا للتوسع في الاستثناءات وقت الأزمات، لذلك تبقى المبادرات المخصوصة والمؤقتة هي الاختيار الأخير في التأطير القانوني لهذه الظروف في ظل الفراغ القانوني الحاصل، ويبقى على البرلمانات عبئ صياغة نصوص أكثر ملاءمة واحتراما للمقتضيات المتعلقة بالحريات الشخصية بالإضافات إلى المراسيم



الحكومية، ثم الاستفادة من التجارب المقارنة الناجحة والممارسات المثلى في هذا المجال، لأجل الوصول الى أطر قانونية مضبوطة غير خاضعة لاستثناءات مؤقتة بحسب الظروف[72].

ويمكن هنا الاستفادة من تجربة هيئات الإغاثة والعون الإنساني التي راكمت تجربة مهمة في التعامل مع بيانات المرضى والمستفيدين من خدمات العون، ولها خبرة في حفظ بيانات الأشخاص والتعامل معها خلال ظروف الأزمات، مثل مكتب الأمم المتحدة لتنسيق الشؤون الإنسانية OCHA، الذي يضم مركزا لتحليل بيانات الأشخاص وله خبرة كبيرة في هذا المجال عبر تأطير التعاون بين الحكومات والشركات والهيئات المدنية والإنسانية، وكذلك لجنة الصليب الأحمر التي أصدرت دليلا مفصلا في مسألة حفظ بيانات الأشخاص في عمليات العون الإنساني، وهو دليل يضم جميع التفاصيل حول المعطيات الشخصية ابتداءا من حمايتها ومشاركتها وتصنيفها وحفظها، ويضم الدليل في جزئه الثاني كذلك كيفية الاستفادة من البرامج الهاتفية والخدمات السحابية والبصمات الرقمية وكيفية معالجة هذه البيانات الشخصية وانتهاء بكيفية التخلص منها[73].

ثم هناك الهلال الأحمر الهولندي، حيث أسس فريق من المتخصصين في مجال الابتكار وعلوم المعلومات في ميدان العمل الإنساني[74] دليلى للسياسات بعنوان «سياسة مسؤولية البيانات» (510 Data Responsi- bility Policy) والتي تنص على مبادئ كالتالي[75]:

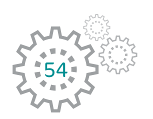
- ضرورة حماية البيانات
- المشروعية القانونية

72. Zwitter A (2012) The rule of law in times of crisis - a legal theory on the state of emergency in the liberal democracy. Archiv Für Rechts- Und Sozialphilosophie 98(1):95–111.

73. Ali A, Qadir J, ur Rasool R, Sathiaseelan A, Zwitter A, Crowcroft J (2016) Big data for development: applications and techniques. Big Data Anal 1(1):1–24. https://doi.org/10.1186/s41044-016-0002-4.

74. Veen, Maarten Van Der (n.d.) Data responsibility V2.2 – 510 global. https://www.510.global/data-responsibility-v2-2/. Accessed 30 Mar 2020.

75. Zwitter A, Boisse-Despiaux M (2018) Blockchain for humanitarian action and development aid. J Int Hum Action 3(1):16. https://doi.org/10.1186/s41018-018-0044-5.



- منع الضرر والإضرار
- احترام حقوق مالكي البيانات
- تحديد الغرض من استخدام هذه البيانات
- تقليص وتقليل البيانات ما أمكن
- الدقة في تحري البيانات وضبطه

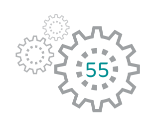
2. المحددات القانونية المُوجِّهة لاستخدامات الذكاء الاصطناعي

في خضم هذا الاستخدام المكثف لتقنيات الذكاء الاصطناعي، تطفو على الساحة قضايا مستجدة متعلقة بمصير البيانات الضخمة التي يتم استخدامها ووجوب حمايتها ضد انتهاكات الخصوصية الشخصية، وقد اصطدمت هذه التقنية بحواجز قانونية تحول دون انتهاك البيانات الشخصية لأجل تغذية بياناتها، وهو الأمر الذي يؤدي إلى تقليل كفاءة أداء هذه التقنية في القيام بأدوارها بشكل فعال، ما يعني عدم إمكانية الإطلاع على بيانات الأشخاص المصابين لأجل جعلها مدخلات للذكاء الاصطناعي كما حدث في الولايات المتحدة، مما يحتم على خوارزميات الذكاء الاصطناعي الاكتفاء بما لديها من بيانات لأشخاص وافقوا على إظهار بياناتهم لأجل استخدامها، الأمر الذي يحد من قدرة الخوارزميات على تحديد خصائص COVID-19 الجديدة التي تظهر في بعض المرضى الذين لا يريدون كشف بياناتهم[76].

وتقوم هيئة قانون نقل التأمين الصحي والمساءلة بحماية معظم بيانات (Health Insurance Portability and Accountability Act (HIPAA))[77] كل مستخدميها، وكذلك تشتغل كل هيئات التأمين حيث تحرص على حجب بيانات زبائنها في المستشفيات وغيرها من مؤسسات الرعاية الصحية، وأي توظيف لهذه البيانات لايمكن أن يتم إلا بعد موافقة الشخص المعني إلا

76. https://www.socialeurope.eu/artificial-intelligence-healthcare-and-the-pandemic.

77. Health Insurance Portability and Accountability Act https://www.hhs.gov/hipaa/index.html.



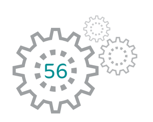
في بعض الحالات النادرة، وتقع كل الهيئات التي تخالف هذا الإجراء تحت طائلة المتابعة قانونية والتغريم، خصوصا وأن الولايات المتحدة لا تتوفر على قانون فدرالي جامع يؤطر مسالة الخصوصية، بل لكل ولاية قوانين حماية الخصوصية الخاصة بها، ما يعني غياب أي إطار قانوني جامع يحدد المعلومات الممكن الاطلاع عليها من تلك المحمية بموجب القانون، وإن كان هذا الاشتباك القانوني يقع لصالح الفرد إلا أنه يكبح قدرة الذكاء الاصطناعي عن الولوج إلى معلومات جوهرية وضرورية لأجل مواجهة هذه الأزمة الصحية العالمية[78].

يبقى النظام الأوروبي العام لحماية البيانات GDPR متقدما وأكثر الأنظمة القانونية تشددا في حماية البيانات الشخصية للمواطنين، ويفرض غرامات مالية لأي استخدام لبيانات الأشخاص دون إذن منهم، ويسري هذا النظام القانوني على أي مؤسسة موجهة لمواطني الاتحاد الأوروبي سواء داخل ترابه أو خارجه، ما جعل هيئات حماية البيانات الشخصية أمام تحدد كبير في هذه الأزمة يكمن في كيفية التعاطي مع هذه المعطيات.

غير أن كلا النظاميين GDPR وHIPAA يضمان بعض الاستثناءات الخاصة في الكشف عن بيانات الأشخاص في الحالات الطارئة المتعلقة بإنقاذ حياة الأشخاص أو تلك المرتبطة بالمصلحة العامة، ولم يتم بعد التنصيص على أحوال خاصة تستهدف جعل هذه البيانات في خدمة الذكاء الاصطناعي، لذلك فمن المرتقب أن يساعد COVID-19 على تعزيز النصوص القانونية المتعلقة بولوج هذه البيانات وتصنيفها في أوقات الجوائح والأوبئة[79].

وينبغي أن نذكر هنا أن البيانات الشخصية الممكن استخدامها غير مقتصرة على الموقع الجغرافي وإنما وإنما حتى المعلومات الجينية والمحادثات الشخصية ومراقبة نشاط مواقع التواصل الاجتماعي وغيرها... كلها

78. https://www.theglobeandmail.com/business/article-platforms-struggle-to-keep-up-with-moderating-content-amid-covid-19/.
79. https://www.insideprivacy.com/covid-19/bipartisan-bill-introduced-in-senate-would-regulate-covid-19-apps/.



بيانات تغذي الذكاء الإصطناعي وتساعده على محاصرة الوباء، لكن يبقى لهذه المعطيات ثمن على حسب حرية الأشخاص وخصوصياتهم.

وقد قام الاتحاد الأوروبي والولايات المتحدة بتقديم مقترحات ودراسات خاصة حول الجوانب القانونية المنظمة لعلاقات حماية البيانات بالذكاء الإصطناعي، لكنها تبقى مقترحات ونصوص غير ملزمة، مما سيجعل من الوباء الحالي دافعا لأجل القيام بإجراءات من قبيل :

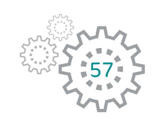
- إصدار قوانين خاصة بخوارزميات الذكاء الإصطناعي للسماح لها بولوج بيانات المرضى لأغراض طارئة، لتعقب انتشار الوباء ثم لزيادة حالة الجاهزية والتأهب إبان فترات الطوارئ دون انتهاك أنظمة الخصوصية الحالية.
- مشاركة الولوج إلى بيانات المرضى لتيسير حالة التأهب والجاهزية في البلدان المصابة من أجل الحد من انتشار المرض.

ومن شأن السماح لولوج هذه البيانات المحمية أن يقلل من انتشار الوباء من خلال تنبيه أسرع للدول وتحكم أكثر في سفر الأشخاص وانتقالهم، مما سيساهم في التعجيل بإيجاد علاجات وبالتالي تحسين حالى المرضى.

إن إنشاء إطار تنظيمي جديد أقل تشددا في حماية البيانات الشخصية قد يشكل مشكلة أخلاقية حقيقية، إذ أدى سوء استخدام هذه البيانات من طرف الشركات في الولايات المتحدة والاتحاد الأوروبي إلى أكبر موجة تغريم وتقاضي وتنازع في تاريخ الولايات المتحدة والاتحاد الأوروبي، ما أدى إلى تنامي المخاوف المعادية لاستخدامات الذكاء الإصطناعي في فترة الجائحة[80].

وهنا يبرز الدور المحوري للتعاون بين الشركات والهيئات التنظيمة الذي من شأنه أن يؤدي إلى إبداع أساليب تنظيمية أكثر مرونة، تدعو من

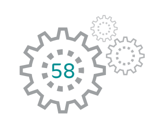
80. https://medium.com/opendatacharter/open-covid-19-data-461e1cbefbba.



خلالها إلى تيسير الامتثال للقواعد الحامية للبيانات الشخصية، فقد كشف التشابك الحاصل في الأنظمة القانونية الحامية للخصوصية في الولايات المتحدة الأمريكية والاتحاد الأوروبي عن الصعوبة الحاصلة في التزام الشركات بهذه القوانين الصارمة، ومن منظور الالتزام والمسؤولية وهناك تيار يدافع عن حماية الشركات من المتابعة القانونية من تبعات سوء استخدام البيانات الشخصية في الذكاء الإصطناعي في الأغراض السليمة في وقت الأزمات، مما سيجعل هذه الحماية القانونية سابقة في تاريخ الشركات الحافل بقضايا المتابعة القانونية بسوء استخدام البيانات الشخصية للزبناء، وقد عبرت الشركات في الولايات المتحدة عن امتعاضها من القيود القانونية المكبلة لها لأجل مواجهة وباء COVID-19، ما حدا بالمشرعين في الولايات المتحدة والمملكة المتحدة تفضيل التساهل التنظيمي المؤقت تجاه هذه الشركات إبان هذه الأزمة الصحية، ما يبين الحاجة إلى التعاون من المشرعين والشركات لأجل خلق توازن عبر منح استثنائات متعلقة باستخدام البيانات ذات الفائدة لمواجهة الجائحة تحت شروط خاصة مع وجوب تحلي الهيئات الرقابة باليقظة والرقابة الدائمة لهذه الشركات[81].

لا يجادل أحد في الدور الهام الذي من شأن تقنيات الذكاء الإصطناعي أن تضطلع به في مواجهة الأوبئة والجوائح، ما من شأنه تثوير استجابة الدول لهذه التحديات الجديدة، لكن الموانع الحائلة أمام هذه التقنية دون الولوج إلى البيانات الضخمة للأشخاص والمرضى التي تمثل مدخلات اشتغالها، تمثل عائقا حقيقيا أمام حسن اشتغالها و مردوديتها.

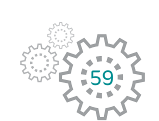
81. https://blogs.worldbank.org/opendata/tfscbs-rapid-support-help-countries-respond-covid-19-outbreak.



الخاتمة : هل حان موعد وداع الخصوصية ؟

إن الاعتماد على قدرة التعلم الآلي التي تتميز بها تقنيات الذكاء الاصطناعي له تبعات أخرى، فهذه تقنيات تتغذى وتتعلم من خلال بيانات الأشخاص وتتبع حالاتهم، لكن أي تشخيص خاطئ من قِبَل هذه الأجهزة للأشخاص من شأنه أن يؤدي إلى اقتراح تشخيص خاطئ، لنكون هنا أمام وجوب تحمل المعالج مسؤوليته في تشخصيه الخاطئ، غير أن السؤال المطروح هنا : لمن تؤول المسؤولية عن التشخيص والعلاج الخاطئين ؟ هناك من يُنزِّه تقنيات الذكاء الاصطناعي عن الخطأ ويسرد في ذلك براهين وسوابق، فإذا كنا في حالة الطبيب نلجأ إلى القواعد المنظمة التي تؤطر مهنة الطبيب وتضبط مسؤولياته فإننا في حالة الروبوت أو التطبيقات الذكية نكون أمام عجز المنظومة القانونية عن الإحاطة بهذه الحالات، بالإضافة إلى إشكالية ترتيب المسؤوليات الملقاة على الطرف المخطئ، لأن تكلفة العلاج الخطأ مكلِّفة لأرواح المرضى ولميزانية الدولة المخصصة للقطاع الصحي، زيادة على أن عملية التشخيص والعلاج لدى الإنسان ليست عملية حَدِّية جامدة خاضعة لقواعد صارمة، ولا تحكمها المعادلات الكيميائية والجرعات الدوائية فقط، لأن الإنسان زيادة على حاجته إلى الذكاء العقلي هو في حاجة إلى ذكاء عاطفي يوفر المناعة النفسية والروحية للمريض، ما يضاعف من حظوظ العلاج والتعافي ويصون معنوياته، هذا الذكاء العاطفي يعدم وجوده لدى الروبوتات والأجهزة الذكية مهما حاولنا محاكاته.

ومنذ عهد أبقراط مبدع القسم المشهور للأطباء إلى الآن، تُلقَّن أخلاقيات ممارسة مهنة الطب في كليات الطب بحيث يحرص الأطباء على واجب حفظ أسرار المريض وصون خصوصيته، لكن هل بمقدور خوارزميات الذكاء الاصطناعي أن تلتزم بأخلاقيات الطبيب ؟ فالتقنيات المستخدمة للمرضى باستطاعتها تتبع وضعهم طيلة اليوم والأسبوع لأجل توقع حالتهم الصحية واستباق الحالات الحرجة منها بالعلاج ـ وهي مسألة إيجابية ـ غير أنه ينبغي الحرص على حسن توظيف هذه البيانات

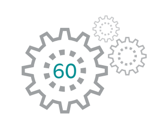


الشخصية للمرضى بحيث لا تُمنح لطرف آخر سواء كان شركة تأمين أو علاج أو دواء أو إشهار.

إن أموراً من قبيل التعاطف والدعم النفسي والحرص على رفع معنويات المريض هي أمور لا تقل أهمية عن مطلب العلاج، ولا نجادل هنا في القدرات المتقدمة لبرمجيات الذكاء الاصطناعي وخوارزمياته، لكن من المستحيل أن نجعل من الروبوتات والبرمجيات أجساما تحاكي الإنسان في تعاطفه وتفهمه ورحمته وكل القيم النبيلة التي يجسدها الإنسان، وليس في هذا إنكار لفائدة الذكاء الاصطناعي أو تنقيص من قيمته كأداة مساعدة في الميدان الصحي، غير أننا قبل أن نوغل في استخدام هذه الخوارزميات لا بد لنا من الحسم في بعض الإشكالات القانونية المتعلقة باستخداماته لأجل الحد من مخاطره، فهل للبرمجيات قَسَمٌ وضوابط أخلاقية تحكم اشتغالها كما للأطباء ضوابط ؟ وإن كان للبرمجيات أخلاقيات وضوابط، فما الذي يُلزِمها أو يجبرها على الالتزام بها ؟

ومن جهة أخرى فإن الاستعمال المتعاظم للتقنيات الذكية للتتبع والمراقبة خلال فترة الوباء والصلاحيات التي منحت للحكومات في استعمال كل الوسائل المتاحة للحد من انتشاره فيها تهديد لحقوق الإنسان وحرياته، الأمر الذي حذا ببعض الخبراء للقول بأننا إزاء أكبر موجة تعقب اجتماعي وملاحقة للمرضى يشهدها العالم، عبر نشر كل الوسائل التكنولوجية الكفيلة بتحقيق هذا الغرض، وهناك تخوف متعاظم بشأن انتهاكات حقوق الانسان كالتشهير والتمييز والعنف والعنصرية... وبالتالي فإن التساهل في الحفاظ على البيانات الشخصية للأفراد ونشر المعلومات والهويات من شأنه أن يسبب مشاكل كبيرة سواء على المدى المتوسط أو البعيد، وقد اعتبر تقرير للهيئة الهولندية لحماية البيانات Dutch DPA[82] أن استعمال تطبيقات تتبع الاتصال يشكل انتهاكا طويل الأمد للحق الأساسي في الحياة الخاصة للمواطنين،

82. https://autoriteitpersoonsgegevens.nl/nl.

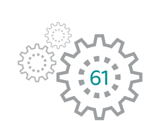


خصوصا وأنه يعالج معطيات لها علاقة بصحة المريض وهي تدخل في خانة البيانات الحساسة.

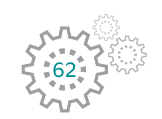
وبما أن الظرف الحالي قد فرض استعمال مثل هذه التطبيقات، فالمخواف تثور من الاستمراري في استعمال وسائل التعقب بعد انقضاء فترة المرض، والسؤال الذي يطرح هنا هل سيتم الاستغناء عن وسائل التتبع والمراقبة بعد انقضاء المرض أم سوف يتم الإبقاء عليها ؟

وهنا تكمن الحاجة إلى رسم خطوط واضحة المعالم توازن بين حق الإنسان الأصيل في الحرية و حاجة الدولة إلى حماية أفرادها وسلامتهم، ويبدو السياق العالمي الحالي مواتيا للتفكير في هذه الإشكالية بالنظر لما يشهده من موجة مراقبة شاملة، خاصة إذا ما علمنا توجه أصحاب القرار إلى التساهل في فرض القيود عن حماية بيانات الأشخاص عوض التشديد على حمايتها، تحت دواعي التنفيس عن الاقتصاد ومسارعة الزمن لإرجاع الوضع إلى حالته الطبيعية كما كان عليه قبل الوباء، ويمكن أن نخلص هنا إلى بعض الملاحظات والتوصيات :

- إن الحاجة إلى المراقبة والتتبع ينبغي أن تقتصر على بيانات الأفراد الشخصية وحياتهم الشخصية بما يخدم حاجة الحفاظ على الصحة العامة فقط دون أن يتجاوزها إلى ما دون ذلك، لأجل صد أي تسريب لهذه البيانات الشخصية أو توظيفها دون إذن رسمي أو مسوغ معقول وسليم.
- التماس الشفافية في الإفصاح عن الطرق التي تشتغل بها هذه التقنيات وإعلام المواطنين بغرض هذه التقنيات وسبل توظيفها لأجل محاصرة الوباء، بحيث يصبح كل المواطنين على اطلاع بخطط الحكومات وأغراض توظيف تقنيات التتبع، وهذا ما ينمي الحاجة إلى تقوية التواصل بين الحكومات والأفراد بلغة بسيطة وواضحة، ما من شأنه تقوية الثقة بين المواطنين وحكوماتهم لأجل إشراكهم لتحقيق تعاون أوسع لكل جهود المجتمع.



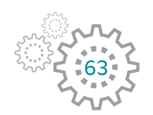
- تحديد الفترة الزمنية اللازمة التي سيتم فيها توظيف تقنيات التتبع والرصد ومواعيد الاستغناء عنها، وتقديم ضمانات عادلة ومقنعة لدفع أي سوء توظيف لهذه المعطيات الشخصية بحيث يقتصر مقدار التدخل في معطيات الأفراد الشخصية على ما يحقق غاية صد الوباء فقط وحصريا دون سواه.
- ينبغي الحرص على حسن توظيف هذه البيانات الشخصية للأفراد بما يخدم غاية صدّ الوباء والسهر على حماية هده المعطيات من أي استغلال أو إيذاء أو انتهاك لحرمة الحياة الشخصية للأفراد، بحيث إن توظيف هده البيانات من قبل أجهزة وأشخاص آخرين بغض النظر عن فائدتها، من شأنه هدم الثقة العامة الضرورية لمواجهة مثل هذه الظروف.
- اعتماد مقاربة متعددة التخصصات عوض المقاربة العلمية الجامدة لموضوع الذكاء الاصطناعي، ومن المهم هنا تشكيل فُرُق متعددة التخصصات يمكنها أن تنظر في عواقب هذه الاختراعات والأنظمة التكنولوجية على المجتمع.
- تمويل الأبحاث التي تعمل على تطوير تطبيقات تجعل من حماية الخصوصية أولوية قصوى ضمن اشتغالها.



لائحة المراجع

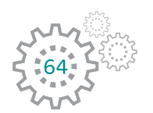
▪ الكتب :

- David K. Linnan ,'Legitimacy, Legal Development and Change: Law and Modernization Reconsidered', Routledge, Apr 22, 2016
- Fotios Fitsilis, 'Imposing Regulation on Advanced Algorithms', Springer Nature, Sep 3, 2019
- Jacob Turner, 'Robot Rules: Regulating Artificial Intelligence', Springer, Oct 29, 2018.
- Kelly Hannah-Moffat, 'Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates', Theoretical Criminology, 2018.
- Kevin Ashley, 'Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age', (Cambridge University Pres, 2017)
- Marcelo Corrales, Mark Fenwick, Nikolaus Forgó ,'Robotics, AI and the Future of Law', Springer, Nov 2, 2018.
- Paul Gowder, 'Transformative legal technology and the rule of law', University of Toronto Law Journal, 68(Supp 1)(2017).
- Paula Boddington, 'Towards a Code of Ethics for Artificial Intelligence' Springer, Nov 9, 2017.
- Richard Susskind, 'Tomorrow's Lawyers: An Introduction to Your Future' (Oxford University Press, 2nd Edition, 2017).
- Tale Skjølsvik, Karl Joachim Breunig, and Frida Pemer, 'Digitalization of Professional Services: The Case of Value Creation in Virtual Law Firms', in Andersson, Per Movin, Staffan Mähring, Magnus Teigland, Robin Wennberg, Karl (Red.),Managing Digital Transformation. (2018)
- The Ethics of Artificial Intelligence: Mapping the Debate" by Brent Daniel Mittelstadt et al. (Big Data & Society, 2016).
- Thomas Wischmeyer, Timo Rademacher, 'Regulating Artificial Intelligence' Springer Nature, Nov 29, 2019.
- Toward an ethics of algorithms: Convening, observation, probability, and timeliness by Ananny, M. (Science, Technology, and Human Values, 2016)



▪ المقالات العلمية :

- Ali A, Qadir J, ur Rasool R, Sathiaseelan A, Zwitter A, Crowcroft J (2016) Big data for development: applications and techniques. Big Data Anal 1(1):1–24. https://doi.org/10.1186/s41044-016-0002-4
- Artificial Intelligence against COVID-19: An Early Review. Medium. (2020). Retrieved 24 April 2020, From https://towardsdatascience.com/artificial-intelligence-against-covid-19-an-early-review-92a8360edaba
- Balkin, Jack M., Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation (September 9, 2017). UC Davis Law Review, (2018 Forthcoming); Yale Law School, Public Law Research Paper No. 615. Available at SSRN: https://ssrn.com/abstract=3038939
- Frank Pasquale, 'A Rule of Persons, Not Machines: The Limits of Legal Automation', 87(1) George Washington Law Review 87(1) (2019).
- Pneumonia of unknown aetiology in Wuhan, China: potential for international spread via commercial air travel,Journal of Travel Medicine, Volume 27, Issue 2, March 2020, From https://academic.oup.com/jtm/article/27/2/taaa008/5704418
- Shuai Wangand athers," A deep learning algorithm using CT images to screen for Corona Virus Disease (COVID 19)", From https://www.medrxiv.org/content/10.1101/2020.02.14.20023028v5.full.pdf+html
- Wachter, Sandra and Mittelstadt, Brent, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI (October 5, 2018). Columbia Business Law Review, 2019(2). Available at SSRN: https://ssrn.com/abstract=3248829
- Zwitter, A., Boisse-Despiaux, M. Blockchain for humanitarian action and development aid. Int J Humanitarian Action 3, 16 (2018). https://doi.org/10.1186/s41018-018-0044-5.
- Zwitter, A., Gstrein, O.J. Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. Int J Humanitarian Action 5, 4 (2020). https://doi.org/10.1186/s41018-020-00072-6



- Zwitter, Andrej, The Rule of Law in Times of Crisis - A Legal Theory on the State of Emergency in the Liberal Democracy (December 1, 2012). Available at SSRN: https://ssrn.com/abstract=2369335 or http://dx.doi.org/10.2139/ssrn.2369335

الاتفاقيات الدولية :

- الإعلان العالمي لحقوق الإنسان
- العهد الدولي للحقوق المدنية والسياسية
- الاتفاقية الأوروبية لحقوق الإنسان
- اتفاقية حقوق الطفل: المادة 16
- الاتفاقية الدولية لحماية جميع العمال المهاجرين وأفراد أسرهم : المادة 14
- الاتفاقية الأمريكية لحقوق الإنسان : المادة 11
- اتفاقية حماية الأفراد فيما يتعلق بالمعالجة التلقائي للبيانات للشخصية :

http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

- البروتوكول الإضافي لاتفاقية حماية الأفراد فيما يتعلق بالمعالجة التلقائية للبيانات الشخصية، فيما يتعلق بالجهات المشرفة وتدفقات البيانات عبر الحدود :

http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181

- بروتوكول تعديل اتفاقية حماية الأفراد فيما يتعلق بالمعالجة التلقائية للبيانات الشخصية :

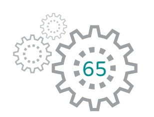
https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/223

- إعلان القاهرة لحقوق الإنسان في الإسلام: المادة 18

http://www1.umn.edu/humanrts/instree/cairodeclaration.html

- الميثاق العربي لحقوق الإنسان : المادتان 16 و21

https://www1.umn.edu/humanrts/instree/loas2005.html



• إعلان مبادئ اللجنة الأفريقية لحقوق الإنسان والشعوب بشأن حرية التعبير في أفريقيا

http://www1.umn.edu/humanrts/achpr/expressionfreedomdec.html

• الميثاق الأفريقي لحقوق ورفاهية الطفل : المادة 19

http://www.au.int/en/sites/default/files/Charter_En_African_Charter_on_the_Rights_and_Wlefare_of_the_Child_AddisAbaba_July1990.pdf

• إعلان حقوق الإنسان لرابطة أمم جنوب شرق آسيا : المادة 21

http://www.asean.org/news/asean-statement-communiques/item/asean-human-rights-declaration

• إطار خصوصية التعاون الاقتصادي لآسيا والمحيط الهادئ :

http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

• توصية مجلس أوروبا رقم 5 (99) R لحماية الخصوصية على الإنترنت :

https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2732155&SecMode=1&DocId=396826&Usage=2

▪ دلائل توجيهية :

• دليل حماية البيانات الخاص بالاتحاد الأوروبي

http://ec.europa.eu/justice/data-protection/index_en.htm

• نشرة وقائع الاتفاقية الأوروبية لحقوق الإنسان حول حماية البيانات الشخصية

http://www.echr.coe.int/Documents/FS_Data_ENG.pdf

• نشرة وقائع الاتفاقية الأوروبية لحقوق الإنسان حول التقنيات الحديثة

http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf

• السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان

https://www.echr.coe.int/Pages/home.aspx?p=home&c

• المبادئ التوجيهية لحماية الخصوصية وتدفقات البيانات الشخصية عبر الحدود :

https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf





شارع الجيش الملكي ـ حي الرياض ـ ص. ب. 2275 ـ ر. ب. 10104،
الرباط ـ المملكة المغربية

الهاتف : 52 60 56 537 (212)+
الفاكس : 12/13 60 56 537 (212)+

البريد الإلكتروني المركزي للإيسيسكو : contact@icesco.org

www.icesco.org